CLOUDERA

WHITE PAPER

CLOUD CONCENTRATION RISK II: WHAT HAS CHANGED IN THE PAST TWO YEARS?

Dr. Richard L. Harmon, Managing Director-Financial Services

Table of Contents

Introduction

> "We are moving towards a world where there is a highly regulated industry that is running on non-regulated third-party infrastructure."
>
> Anonymous CTO—G-SIB

The above statement summarizes how profoundly the Financial Services industry will be transformed by cloud computing in five years. This seismic change will drive new innovations but concurrently introduce new types of risks that need to be addressed by regulators, the Financial Services industry and technology innovators.

It has been two years since I wrote my first paper on Cloud Concentration Risk[1] and much has changed since then. First, more regulators have begun to explore this topic and are evaluating the potential operational and financial stability risks from the industry's accelerating movement to the cloud. Second, several global systemically important banks (G-SIBs) have also taken note and are beginning to consider this as a new factor within their operational risk frameworks. Their primary focus is on concerns related to vendor lock-in, consistent data governance and data security when adopting a multi-cloud strategy rather than the wider systemic risk exposures. Finally, the Big Data space has seen significant innovation and consolidation which has enabled Cloudera, after the merger with Hortonworks, to focus on developing the next generation Enterprise Data Cloud Platform.

This paper will provide a brief overview of key trends in cloud adoption and cloud deployment strategies, how global regulators are evaluating cloud related risks and how might they deal with these potential risks in the future. Furthermore, the role of recent innovations in the Big Data and analytics space provides new capabilities to enable the next generation hybrid, multi-cloud architecture that addresses many of the near-term risks that regulators have identified. What is still outstanding, in my opinion, is the need to tackle the financial stability risks associated with Cloud Concentration Risk.

The last section will put forth a few recommendations for regulators and the wider Financial Services industry to enable enhanced transparency through data gathering and to enable stress testing capabilities to identify contagion trigger points that can result in cloud specific systemic risk events. It is recommended that financial service institutions and regulators consider utilizing the latest simulation technology to help quantify these risks and to evaluate what types of supervisory policies might be most effective to tackle systemic risk exposures.

[1] Harmon, Richard. "Cloud Concentration Risk: Will This Be Our Next Systemic Risk Event?" Cloudera White Paper, May 2018. Cloudera White Paper, May 2018.

Cloud Service Provider (CSP) Offerings

The Cloud environment can be simplified by segmenting this market into three types of services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).[2]

Infrastructure as a Service (IaaS): IaaS delivers cloud computing infrastructure, including servers, network, operating systems, and storage, through virtualization technology. IaaS provides the same technologies and capabilities as a traditional data center without having to physically maintain or manage all the physical components. IaaS clients access their servers and storage directly, but it is all outsourced through a "virtual data center" in the cloud.

IaaS is the most flexible cloud computing service with the following benefits:

- Resources are available as a service
- Cost varies depending on consumption
- Services are highly scalable
- Multiple users on a single piece of hardware
- Institutions retain complete control of the infrastructure
- Dynamic and flexible

Platform as a Service (PaaS): PaaS delivers a framework for developers that they can build upon and use to create customized applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers maintain management of the applications. This platform is delivered via the web, giving developers the freedom to concentrate on building the software without having to worry about operating systems, software updates, storage, or infrastructure.

Software as a Service (SaaS): SaaS utilizes the internet to deliver applications, which are managed by a third-party vendor, to its users. Most SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side.

[2] Scott, Gulliver & Nadler. "Cloud Computing in the Financial Sector: A Global Perspective." Program on International Financial Systems, July, 2019.

Figure 1 provides a clear delineation between the three cloud service offerings.[3] The focus of this paper will be on the IaaS market segment.

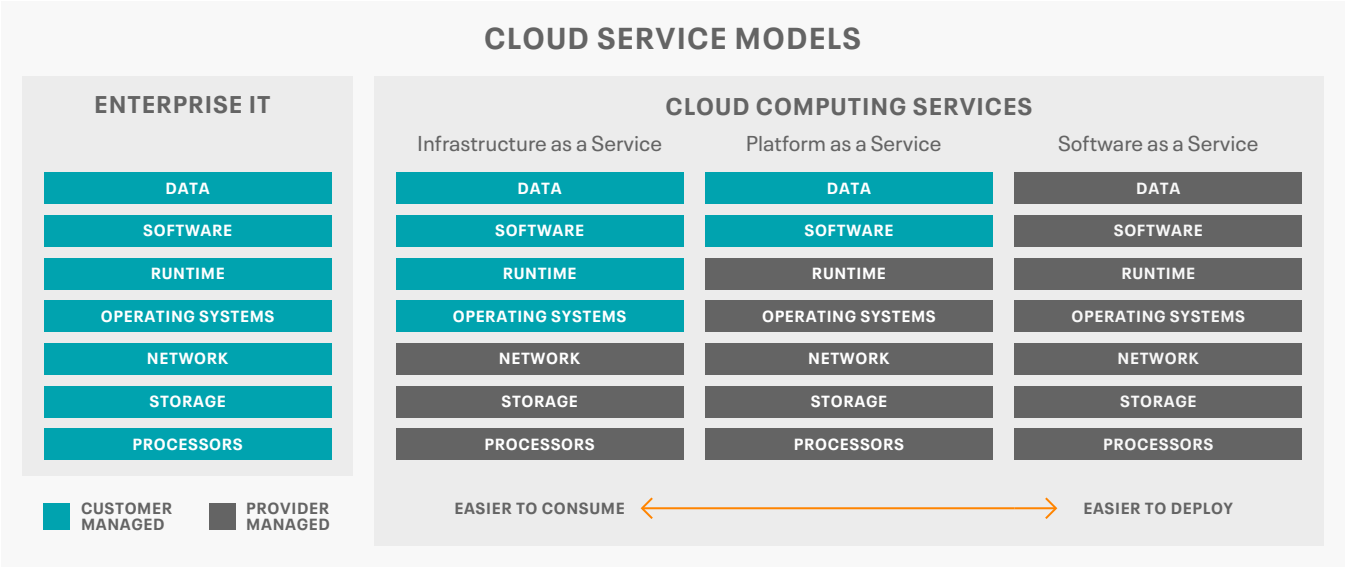

Figure 1

Industry Trends in Cloud Computing

Cloud adoption in financial services has been accelerating over the past few years. Enterprises are after the speed, agility, simplicity, and lower costs that it provides.

The most recent analysis of the global cloud market by Gartner shows that Infrastructure as a Service (IaaS) market grew 31.3% in 2018 to total $32.4 billion, up from $24.7 billion in 2017. As documented in Figure 2, Gartner estimates that Amazon continues to hold the largest market share in the IaaS market in 2018 with a 47.8 percent market share. This is followed by Microsoft, Alibaba, Google and IBM.

[3] Financial Stability Board. "Third-party dependencies in cloud services: Considerations on financial stability implications." FSB Publication, December 9, 2019.

It should be noted that AWS and Microsoft have a combined global market share of 63.3 percent in 2018, a slight increase from their 62.1 percent combined global market share in 2017.

WORLDWIDE IAAS PUBLIC CLOUD SERVICES MARKET SHARE, 2017-2018 (MILLIONS OF US DOLLARS)					
	2018		2017		2018-2017
Company	Revenue	Market Share (%)	Revenue	Market Share (%)	Growth (%)
Amazon	$15 ,495	47.8%	$12,221	49.4%	26.8%
Microsoft	$5,038	15.5%	$3,130	12.7%	60.9%
Alibaba	$2,499	7.7%	$1,298	5.3%	92.6%
Google	$1,314	4.0%	$820	3.3%	60.2%
IBM	$577	1.8%	$463	1.9%	24.7%
Others	$7,519	23.2%	$6,768	27.4%	11.1%
Total	**$32,441**	**100.0%**	**$24,699**	**100.0%**	**31.3%**

Figure 2

Gartner's research vice president, Sid Nag, highlights this trend in his analysis:

> "Despite strong growth across the board, the cloud market's consolidation favors the large and dominant providers, with smaller and niche providers losing share.... This is an indication that scalability matters when it comes to the public cloud IaaS business. Only those providers who invest capital expenditure in building out data centers at scale across multiple regions will succeed and continue to capture market share. Offering rich feature functionality across the cloud technology stack will be the ticket to success, as well."[4]

[4] Gartner. ""Forecast: Public Cloud Services, Worldwide, 2017-2023, 3Q19 Update." November 2019

Regulatory Focus on Third-Party Outsourcing and Operational Resiliency

The growth in cloud adoption across the Financial Services industry and the associated increasing reliance on third party infrastructure providers has gained the attention of regulators at global, regional and national levels.

At a high level, a core regulatory concern is the operational resiliency in the "shared responsibility model" that exists between a cloud customer and the cloud service provider (CSP). Within the context of the IaaS offering, while the CSPs retain responsibility over the lower level layers of infrastructure, the financial institution is responsible for the data stored and processed, the overall security of the solutions developed on the Cloud and the ability to assess the CSP's compliance with required resiliency requirements.[5]

Global Regulators

At the global level, the Financial Stability Board (FSB) and the Bank of International Settlements (BIS) have recently issued a few publications focused on the operational and supervisory risks of third-party cloud service providers. A recent FSB study[6] identified a few notable market trends that highlight operational and financial stability concerns:

- From a survey of 294 global financial service institutions, the respondents exhibited a strong reliance on a narrow set of major cloud service providers
- While currently very limited, the survey noted the accelerating use of cloud services for "core" or critical systems

Based on these trends, FSB identified several areas of concern related to financial stability:

- Operational incidents at third-party service providers may result in temporary outages affecting FIs, and misconfigurations of new tools could result in data breaches
- Concerns about the ability to monitor and manage third-party cloud service provider related operational risks due to contractual limitations on institutions' and regulators' rights of access, audit and information
- Bank resolution authorities may have difficulties when exercising step-in rights in resolution if critical bank data systems are held in third-party systems
- **There are a number of cross-border, cross-jurisdiction related complexities in the oversight of providers and in the management of systemic risks**
- **Potential concentration in third-party provision could result in systemic effects in the case of a large-scale operational failure or insolvency**

[5] David Strachan. "Financial services on the Cloud: the regulatory approach." Deloitte Blog, 16/09/2019.
[6] Financial Stability Board. "Third-party dependencies in cloud services: Considerations on financial stability implications." FSB Publication, December 9, 2019.

I emphasize the last two points since these are key factors that relate specifically to systemic risk exposures.

This is similar for the Insurance sector with a great overview provided by the BIS's Financial Stability Institute in a comparative study of different regulatory approaches globally.[7] Figure 3 is a summary of different regulatory approaches taken to address the insurance sector's use of cloud service providers. As with the banking sector, insurance regulators have not widely addressed cloud-specific outsourcing supervisory requirements beyond the more general outsourcing frameworks.

SUPERVISORY AUTHORITY REGULATIONS, EXPECTATIONS AND STATEMENTS APPLYING TO CLOUD COMPUTING

Frameworks	Outsourcing		Governance & Rick Management		Information Security	
	General	Cloud Specific	General	Cloud Specific	General	Cloud Specific
APRA	■	■	■		■*	
OSFI	■	■			■	
EIOPA			■			
ACRP			■	■		
BaFin			■	■	■	
HKIA	■		■			
IRDAI	■		■		■	■
DNB			■	■		
SAMA	■				■	■
MAS**	■	■			■	■
FINMA	■		■			
FCA	■	■				
PRA			■			
NAIC			■		■	

■ General framework ■ Cloud-specific statement ■ General framework with a specific section on cloud

* Currently under consultation process.

** MAS Outsourcing and Technology Risk Management Guidelines are not legally binding and are used to set out MAS expectations on financial institutions on a non-mandatory basis.

Source: Bank of International Settlements

Figure 3

[7] Bank of International Settlements. "Regulating and supervising the clouds: emerging prudential approaches for insurance companies". FSI Insights on policy implementation, No 13 Dec, 2018.

European Regulators

On the European side, there are several recent publications[8] from the European Banking Authority (EBA), the European Central Bank (ECB), the European Systemic Risk Board (ESRB), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) focused on systemic risk.[9]

The EBA published revised outsourcing guidelines in February 2019 that became effective on September 30, 2019.[10] The key outsourcing requirements consisted of the following:

- The revised guidelines are consistent with current outsourcing requirements within PSD2, MiFID II and the Central Registration Depository (CRD), but extend the scope of the previous Committee of European Banking Supervisors (CEBS) guidelines to cover all banking, payment and investment services
- Each financial institution's management body remains responsible for its activities at all times and must ensure that sufficient resources are applied to the oversight and risk management of all outsourcing arrangements, with particular regard to those that support critical or important functions
- Where the outsourced service provider is located in a third country, institutions must ensure that all EU legislation and regulations are complied with, including, but not limited to, the protection of personal data
- To enable competent authorities to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring associated concentration risks, institutions must be able to provide comprehensive documentation on their outsourcing arrangements

In principle these appear to be one of the most extensive efforts by a regulator to manage perceived risks from cloud service providers.

The ESRB's recently released study on systemic cybersecurity risk noted that:

> "... the adoption of new technologies such as cloud computing creates new interdependencies with entities that may operate outside the boundaries of regulated financial systems."[11]

[8] See References for a representative list of documents published by global, regional and national regulators.
[9] European Banking Authority. "Final Report on EBA Guidelines on outsourcing arrangements." February 25, 2019.
[10] Majithia, Rakesh. "At A Glance: EBA issues revised guidelines on outsourcing." PWC, February 2019.
[11] European Systemic Risk Board. "Systemic cyber risk." ESRB, February, 2020.

Furthermore, the UK House of Commons Treasury Committee[12] noted that the Bank of England, the Financial Conduct Authority and the Prudential Regulation Authority found:

> "At the system level, some third-party providers (including cloud service provides) may be a key point of concentration and present a single point of failure risk where an operational incident could have a widespread impact on the system."

Finally, ESMA has identified a range of regulatory initiatives for Credit Rating Agencies (CRAs) in 2020 with outsourcing to cloud service providers identified as a key focus area:[13]

> "ESMA considers that outsourcing to cloud service providers is a risk that CRAs are not yet managing appropriately. In the course of 2020, ESMA will continue to focus on this risk area to identify any specific concerns and engage with the firms appropriately."

United States Regulators

On the US side, regulatory entities coordinate their supervision of banks and their technology service providers through the Federal Financial Institutions Examination Council (FFIEC), whose members include the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). The FFIEC sets policy regarding the responsibility of various agencies, which service providers get examined, the frequency of examination, and the scope of supervision.[14,15]

[12] UK House of Commons Treasury Committee. 'IT failures in the Financial Services Sector." Second Report of Session 2019-20, October 22, 2019.
[13] European Securities and Markets Authority. "ESMA Supervision—Annual Report 2019 and Work Programme 2020". ESMA, March 9, 2020.
[14] Scott, Gulliver & Nadler. "Cloud Computing in the Financial Sector: A Global Perspective." Program on International Financial Systems, July, 2019.
[15] The Financial Stability Oversight Council (FSOC) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act and created to address the fact that no single regulator had responsibility for monitoring and addressing overall risks to financial stability. In their 2019 Annual Report third-party outsourcing risks were not highlighted as a crucial systemic risk concern.

The Federal Reserve, the US Congress and other policy leaders in the US have started to explore whether the regulators are properly setup to ensure that they have the tools for addressing Cloud Concentration Risk exposures. There has been much discussion on the use of the Financial Stability Oversight Council (FSOC) to designate Amazon Web Services, Microsoft Azure and Google Cloud as "systemically important financial market utilities."[16] This will continue to be a discussion topic with the US regulators looking internationally to address the global systemic risk issue around Cloud Concentration Risk.

In testimony to Congress, Federal Reserve Governor Lael Brainard stated,

> "Certainly there's work internationally where we're thinking about precisely this question that you raise about the ability to fail over... [regulators recognize that] migrating to the cloud mitigates some risks, adds other risks, and so we need to hold our institutions accountable for making that risk assessment in a very well-informed way and taking that migration very seriously."[17]

APAC Regulators

The APAC region is a global leader in many areas of mobile interaction and digital transformation. Regulators overall have been accommodating towards some use of cloud services, but some are still clarifying outsourcing rules and guidelines to help institutions achieve compliance. Generally, the APAC region has more regulatory restrictions on cloud adoption. Very few critical core banking systems currently reside in the cloud. More institutions will slowly begin to migrate to the cloud in the next few years though at a slower pace than in the US or Europe.[18]

The Monetary Authority of Singapore has a consultation on new proposals to expand its regulatory oversight of bank outsourcing arrangements. The new regime will require banks to conduct due diligence checks on technology partners and demonstrate that they have satisfactory safeguards and response plans in place in the event of disruption. Similarly, the Hong Kong Monetary Authority is also enforcing third party vendor risk management guidelines for Financial Services institutions.[19]

[16] Pederson, Brendon. "Does Amazon-Google-Microsoft hold on the cloud pose a risk to banking?" American Banker, September 30, 2019.
[17] Pederson, Brendon. "Does Amazon-Google-Microsoft hold on the cloud pose a risk to banking?" American Banker, September 30, 2019.
[18] Asia Cloud Computing Association (ACCA). "Asia's Financial Services on the Cloud 2018: Regulatory Landscape Impacting the Use of Cloud by Financial Services Institutions in Asia." ACCA, (2018)
[19] BitSight. "Managing risk in an increasingly regulated world". BitSight White Paper (2020)

Similarly, the Australian Prudential Regulatory Authority outlined their oversight role for cloud computing services,

> "When the proposed use of cloud computing services involves heightened or extreme inherent risks, APRA encourages consultation prior to entering into any arrangement, regardless of whether offshoring is involved."[20]

The Brookings—University of Chicago Booth Financial Stability Task Force

Outside of these regulatory efforts there is also a newly formed Financial Stability Task Force setup by the Brookings Institute and the University of Chicago Booth School. This Task Force is composed of top former policy leaders, leading academics and a small select group of business leaders. The Task Force is to identify "financial stability (FS) risks that are not well-handled by the existing financial stability regime in the U.S." One of the topics the Task Force is studying is Cloud Concentration Risk with recommendations on how best to address specific concerns within the United States regulatory framework. Their study and its recommendations should be published later this year.

Systemic Risk and Cloud Concentration Risk Exposures

The previous section highlights a few key examples of the breadth and variety of regulatory approaches being taken to address third party cloud service providers. However, regulators have not yet addressed in sufficient detail specific concerns about potential systemic risk impacts. This is especially true of the risks associated with Cloud Concentration Risk.

Detailed CSP IaaS cloud market share estimates for the Financial Services industry is not publicly released by the CSPs. Fortunately, in January 2020, the Bank of England published some high-level results of an annual survey of the 30 largest banks and 27 largest insurers that they supervise to understand how these institutions utilize the cloud. This includes a good selection of some of the largest global banks since many have significant operations in London.[21]

[20] Australian Prudential Regulatory Authority. "Outsourcing Involving Cloud Computing Services." APRA, Information Paper, September 24, 2018.
[21] Bank of England. "How reliant are banks and i d outsourcing?" Bank Overground, January 17, 2020.

As revealed in Figure 4, the top two providers, AWS and Microsoft, probably have a slightly higher combined market share concentration in the Financial Services industry than Gartner measured across the overall market (see Figure 2).

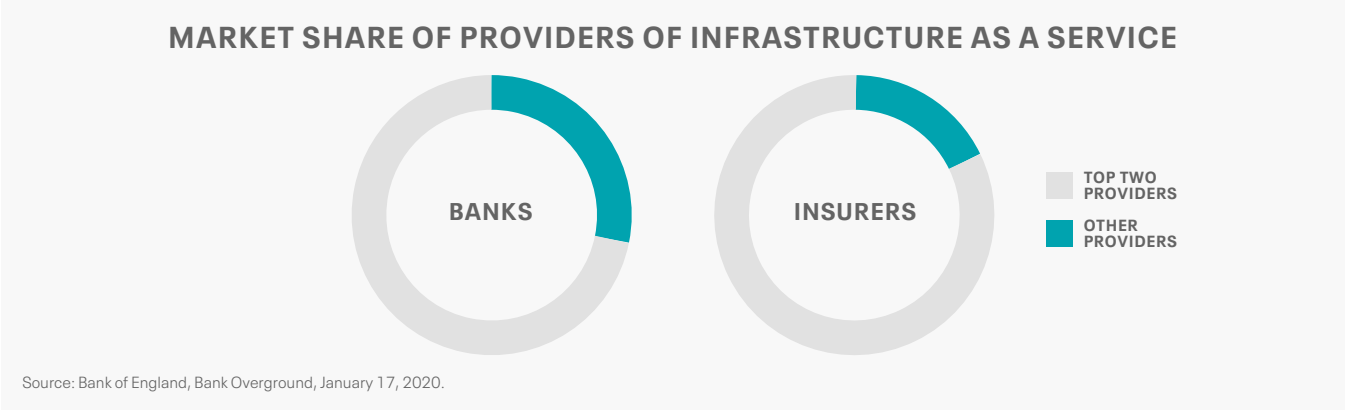

Figure 4

It should be noted that in this publication the Bank of England stated:

> "Our survey indicates that for banks and insurers, the provision of IT infrastructure in the cloud is already highly concentrated."

Furthermore, they mentioned that,

> "We will use the results of the survey to inform and adjust our supervisory approach to cloud oversight."

While a diverse list of operational resiliency concerns has been identified across many regulator publications, I perceive the following six items reflect the most critical factors in evaluating future systemic risk exposures.

1. **Lack of unified data security and governance**—Each cloud native product re-creates its own silo of metadata making data management, security and governance much more complex. Without a unified security and governance framework, institutions will be challenged to identify, monitor and address crucial issues in data management that are critical for proper measurement of risk exposures across different platforms. This is especially true for Hybrid or Multi-Cloud environments.
2. **Cyber attack resiliency**—The consolidation of multiple organizations within one cloud service provider (CSP) presents a more attractive target for cyber criminals than a single organization.[22] A further complication is that Cloud security is a shared responsibility between the CSP and the institution.
3. **Vendor lock-in**—The market share concentration of a small group of cloud service providers can result in significant lock-in effects, whereby an institution is unable to easily change its cloud provider either due to the terms of a contract, a lack of feasible alternatives, proprietary technical features or high switching costs.
4. **Operational resiliency**—Much of the operational resiliency concerns by regulators is the "shared responsibility" model inherent in the relationship between a Cloud customer and the CSP. Regulators have consistently made it clear that institutions at all times remain fully responsible for all the operational functions they outsource to third-party providers. This addresses the liability but does not address the fundamental exposure that still exists.
5. **Lack of transparency**—A cloud service provider (CSP) is unlikely to share detailed information about its processes, operations, and controls. This restricts not only an individual institution but also the regulator from being able to fully ensure sufficient oversight to ensure very limited operational risk exposures as well as the ability of regulatory authorities to properly perform their oversight function. From a reporting perspective, the UK and Luxembourg regulators require institutions to periodically report all functions outsourced to the Cloud, alongside requiring pre-authorization for critical activities.

[22] In 2017, the ESRB established the European Systemic Cyber Group (ESCG) to investigate systemic cyber risk and examine whether and how a cyber incident could cause a systemic crisis. The analysis conducted shows that a cyber incident could indeed evolve into a systemic cyber crisis that threatens financial stability with the potential to have serious negative consequences for the real economy. (Source: ESRB: "Systemic cyber risk", February 2020)

6. **Cloud concentration risk**—Regulators are concerned about institutions' over reliance on one service provider to support their banking services. This not only presents operational risks for individual institutions but creates financial stability risks for the financial system within a single country as well as globally. Concentration risks also arise if a significant number of institutions have a key operational or market infrastructure capability (e.g. payment, settlement and clearing systems) in a single CSP. For instance, there is abundant research and analysis on the potential systemic risk exposures from Central Counterparties (CCPs) and their default fund structures but little discussion among regulators on Cloud Concentration Risk in these risk assessments.

Specifically, with regard to the issue of Cloud Concentration Risk, we can segment this into two distinct categories:

- **Firm-specific concentration risks**—these consist of risks due to cloud lock-in, a lack of unified data security and governance across CSPs, third-party operational resiliency concerns such auditability, multi-cloud controls and cyber security exposures
- **Systemic concentration risks**—these consist of risks that affect the stability of the financial system. This includes a lack of transparency on what critical applications currently reside on or will migrate to a specific CSP. Regulators are also concerned about the systemic risk of having a concentration of many large financial service firms' critical application(s) all reside on the same CSP. For example, these include payment, settlement, and clearing systems.

This bifurcation of oversight complexities of Cloud Concentration Risk highlights the need for the Financial Services industry, the CSPs and regulators to collaboratively work towards resolving these issues.

Fortunately, recent innovations in developing a comprehensive hybrid, multi-cloud architecture, generically referred to as the Enterprise Data Cloud, directly eliminates most of the concerns around vendor lock-in dangers as well as the lack of unified multi-cloud data security and governance capability that in turn helps address some key regulatory concerns of firm-specific Cloud Concentration Risk.

The Enterprise Data Cloud—the Future of Cloud Computing

The previous section highlights a few key examples of the breadth and variety of regulatory approaches being taken to address third party cloud service providers. However, regulators have not yet addressed in sufficient detail specific concerns about potential systemic risk impacts. This is especially true of the risks associated with Cloud Concentration Risk.

A recent Gartner survey across all industries, provides an indication of the movement by the Financial Services Industry towards a hybrid, multi-Cloud framework (Figure 5). Their survey shows that 69% of organizations surveyed express plans to follow a hybrid, multi-cloud strategy.

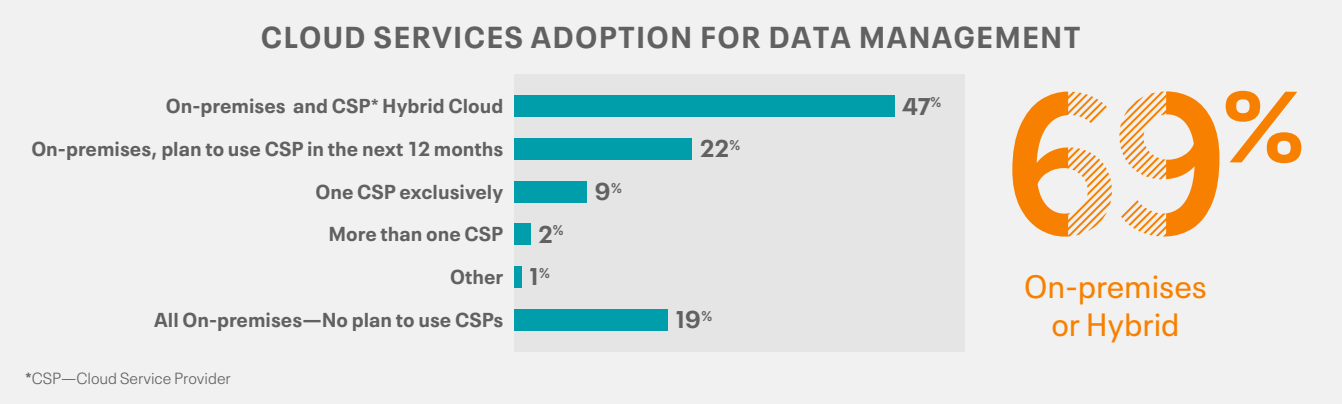

Figure 5

The original Big Data open source platform, Hadoop, has experienced continuous innovation throughout the past decade. The advent of the wide adoption of cloud computing and the need to manage data, workloads and security across many platforms has led to the development of the next generation Big Data platform. At Cloudera we call this hybrid, multi-cloud framework the "Enterprise Data Cloud." Gartner calls this the emergence of "Cloud Data Ecosystems"[23] while 451 Research describes this as "Enterprise Intelligence Platforms."[24] Regardless of the terminology chosen, the clear understanding is that the future of cloud computing will need to support an agile hybrid, multi-cloud environment.

[23] Adrian, Merv. "Stop Talking About 'Hadoop'." Gartner Blog, March 4, 2020.
[24] Ashlett, Matt. "Don't Call It A Comeback: Cloudera Accelerates Its Hybrid Cloud Strategy." 451 Research, March 13, 2020.

Figure 6 provides a simple comparison of the requirements between the first decade of the Big Data platform and some of the distinct requirements needed for the next decade with Big Data powered data clouds.

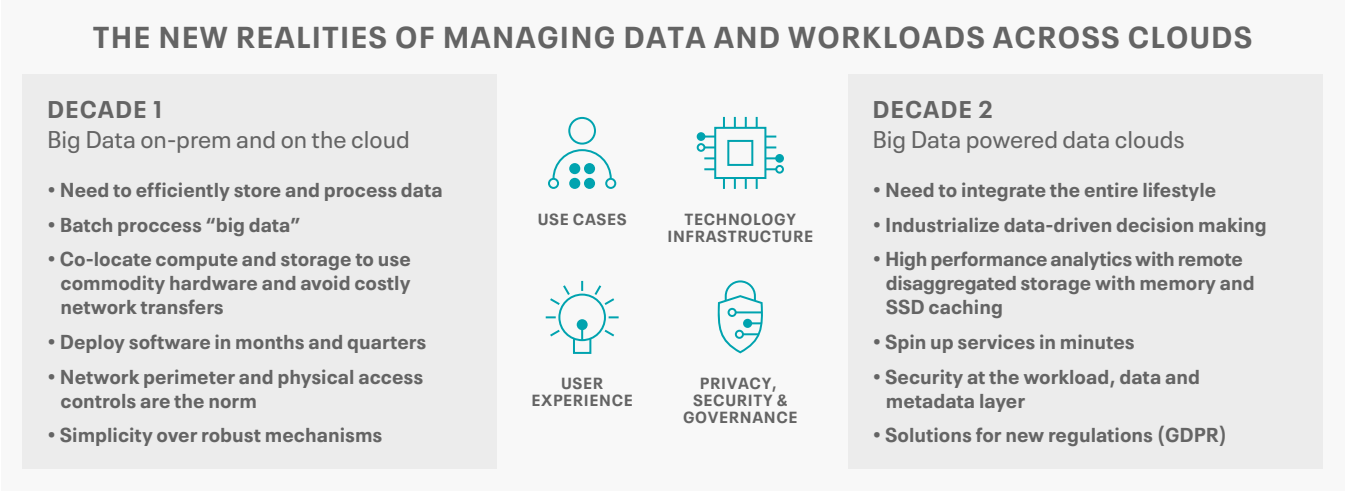

Figure 6

From a high-level perspective, an Enterprise Data Cloud needs to support:

- **Hybrid and multi-cloud**—to provide data management capabilities to manage, analyze and experiment with data in any public or private cloud or on-premise data center for maximum choice and flexibility
- **Multi-function capabilities**—to address the most demanding business use cases requires applying real-time stream processing, data warehousing, data science and iterative machine learning across shared data at scale
- **Secure and governed**—simplifies data privacy, security and compliance for diverse enterprise data with a common security model to govern data on any cloud—public, private and hybrid
- **Open source**—facilitates innovation within the open source community, the choice of open storage and compute architectures without vendor lock-in, and the confidence and flexibility of a broad ecosystem supporting both legacy systems and innovative partners

While hybrid cloud environments bring substantial advantages in terms of rapid deployment and reduced infrastructure costs, they bring a new set of data management challenges.

As cloud environments multiply, new cloud data silos can appear, some of which bypass IT altogether. Securing and governing data that lives across multiple clouds, each with their own architecture is difficult. Furthermore, cloud vendor lock-in effects can make it difficult and costly to migrate or export data.[25]

From a cloud migration perspective, it is important that institutions first develop an enterprise data strategy before finalizing their cloud strategy. This allows institutions to implement their enterprise data strategy consistently in the cloud by focusing on data storage, data management, and data protection requirements. This helps to ensure that a uniform multi-platform security and governance framework is put into place that supports an institution's core business objectives—such as increasing revenue, improving customer satisfaction and protecting the business while driving profitability.

Cloudera is leading the industry in offering the world's first Enterprise Data Cloud. We call this the Cloudera Data Platform (CDP). As illustrated in Figure 7, the Cloudera Data Platform provides three form factors; CDP Public Cloud, CDP Private Cloud and CDP Data Center (the on-premises version of CDP) in a single unified platform that prevents cloud lock-in by delivering the following capabilities:

- **Built-in, enterprise grade security and governance** with Shared Data Experience (SDX). This allows an institution to have a single control plane to secure, govern, and track lineage across the entire data landscape.
- **Complete Data Lifecycle** from data collection, through curation, reporting, to machine learning applications. You can perform all these functions in a single, integrated data platform, reducing the time-to-insight.
- **Open data standards, cloud portability, data independence**. At Cloudera we believe in open source software and open platforms that do not lock customers in proprietary formats and technologies.

[25] Cloudera. "Why a Successful Hybrid Cloud Strategy Requires an Enterprise Data Strategy: Five Strategic Considerations for Hybrid Cloud Success". Cloudera White Paper, January 2020.

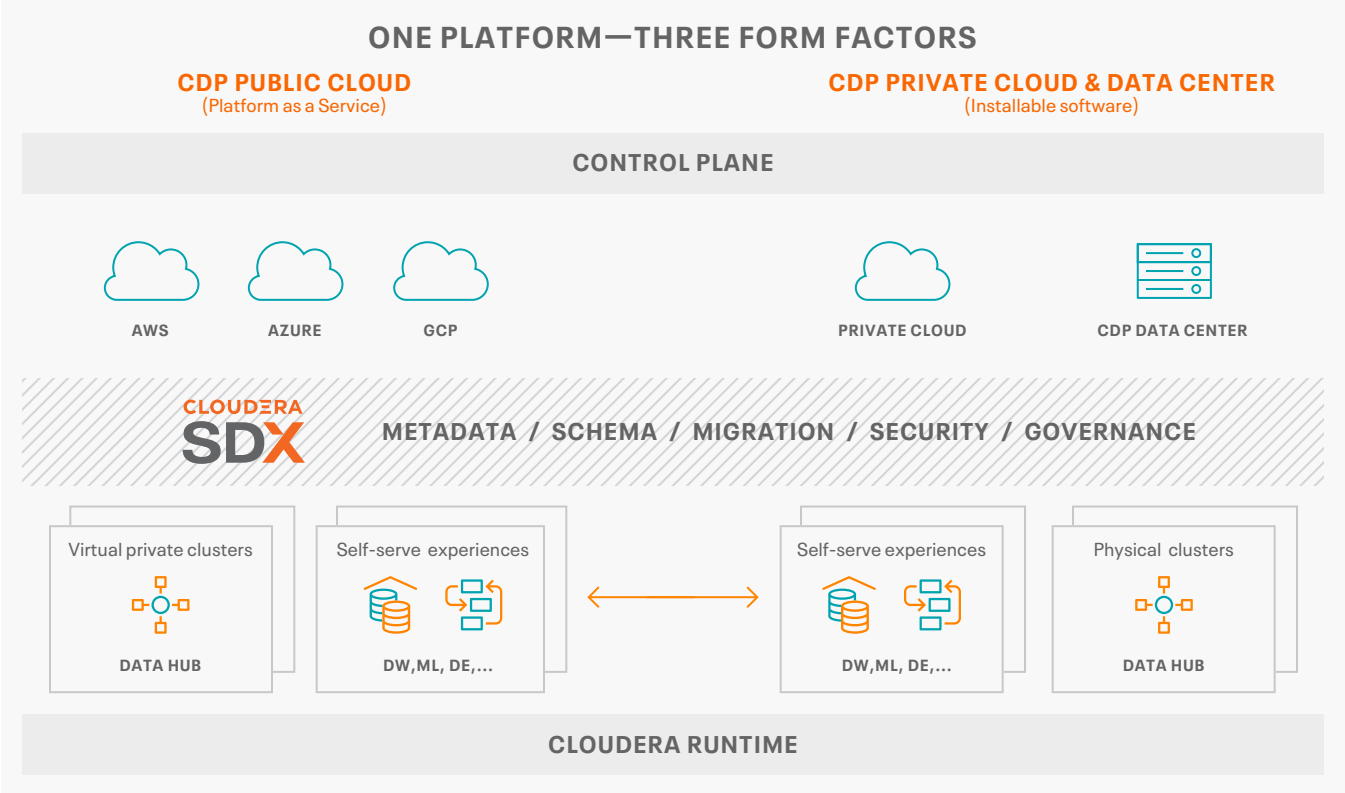

Figure 7

CDP empowers users to get insights from data faster, while not compromising on enterprise security, data governance and lineage. For system administrators CDP provides a single pane of glass to control the entire platform starting from procurement of compute resources on the cloud to managing user access and tracking SLAs. For data stewards and engineers, CDP provides an intuitive user interface to find data assets, profile them, and develop data pipelines to clean and enrich the data. Finally, for data analysts and researchers, CDP gives the choice of compute engines and a choice of tools to query the data, build reports, and develop analytical models.

Evaluating Cloud Concentration Risk Using Simulation

The complex and emergent behavior of financial markets, especially under stress, has proven difficult to model with traditional mathematical approaches. A simulation-based approach that comes out of the complexity science literature is starting to gain traction in Financial Services. This approach is referred to as Agent Based Modelling (ABM). ABM is a bottom-up approach to the modelling of complex and adaptive systems with heterogeneous agents.

A key factor that is not addressed by traditional Machine Learning-based approaches is that the sequencing of events within a period of time can be vitally important for capturing interconnecting effects that develop into trigger points for wider contagion effects. This allows ABMs to explain how the behavior of individual institutions or agents can affect outcomes in complex systems and offers the opportunity to understand potential vulnerabilities and paths through which risks can propagate across the financial system. Additionally, such models offer the ability to depict the heterogeneity of agents, as well as idiosyncratic rules for how financial institutions operate, which are important for replicating real market conditions.[26]

An ABM simulation framework allows regulators and financial services institutions to develop dynamic simulation environments that can evaluate thousands of stress test scenarios at the system-wide level. This can be an indispensable tool to identify and quantify emerging financial stability risks around third party cloud outsourcing and cloud concentration.

As an illustrative example, let's take a simplified example of central counterparties (CCPs) from a concentration risk perspective. Since the 2008-2009 financial crisis there has been a global push for far greater use of central clearing. This has led to an expansion of CCPs over time. In the event of an operational or liquidity disruption within a CCP, all of its clearing members would be impacted. Given that larger financial institutions have memberships in many other CCPs, this disruption can quickly spill over to other CCPs. Figure 8 is from a study completed by Soramaki and Cook (2018) that provides a clear visual representation of CCP interconnectedness.[27]

[26] There are many examples of ABM simulation models developed for systemic risk and policy evaluations. One example that would be similar in design is a paper by Bookstaber, Richard, Paddrik, Mark and Tivanax, Brian. "An Agent-based Model for Financial Vulnerability." Journal of Economic Interaction and Coordination, 2018, vol. 13, issue 2, 433-466.

[27] Soramaki, Kimmo and Cook, Samantha. "Mapping clearing interdependencies and systemic risk." FIA, September 27, 2018.

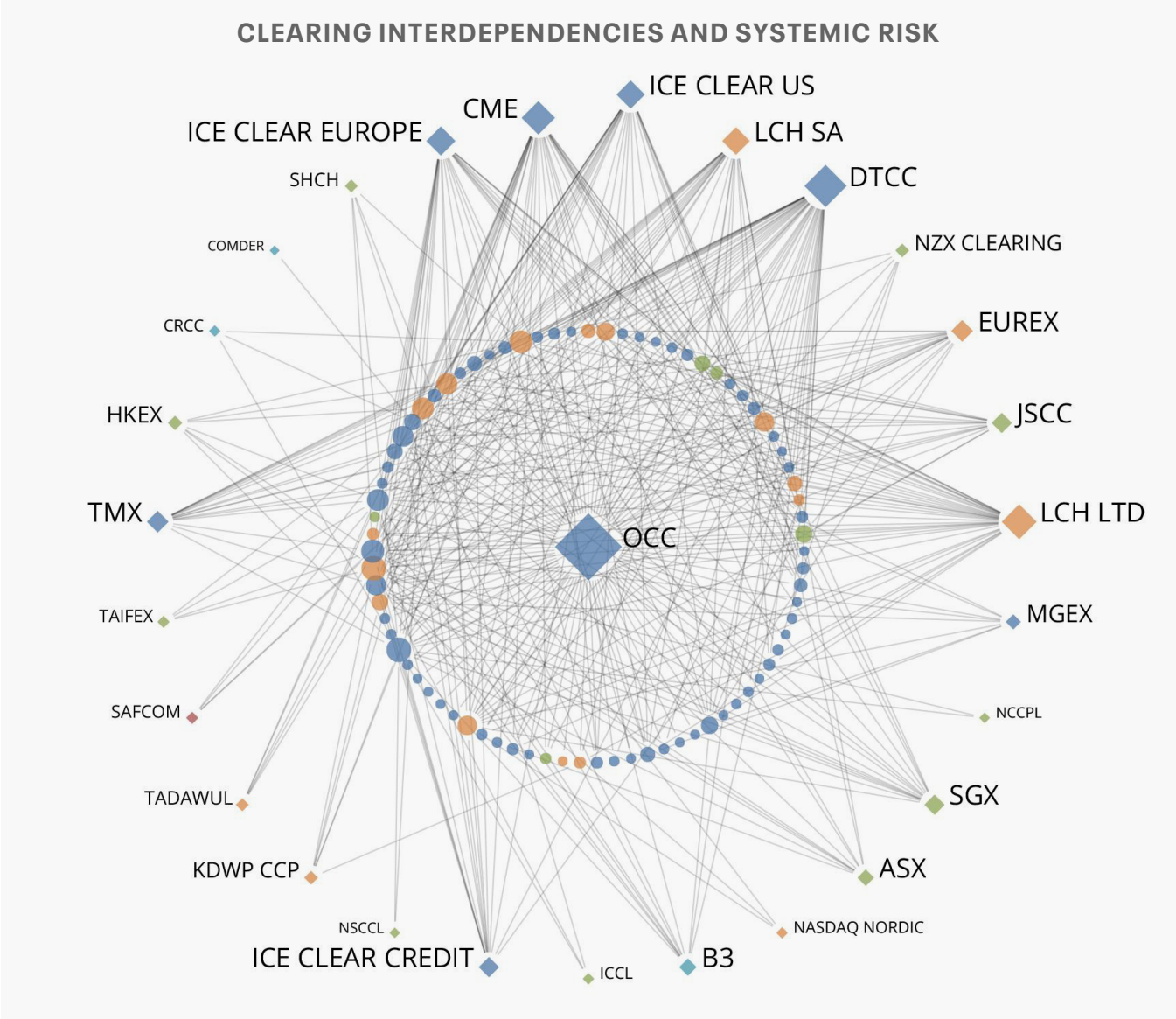
CLEARING INTERDEPENDENCIES AND SYSTEMIC RISK
ICE CLEAR US
CME
ICE CLEAR EUROPE
LCH SA
SHCH
DTCC
COMDER
NZX CLEARING
CRCC
EUREX
HKEX
JSCC
TMX
OCC
LCH LTD
TAIFEX
MGEX
SAFCOM
NCCPL
TADAWUL
SGX
KDWP CCP
ASX
NSCCL
NASDAQ NORDIC
ICE CLEAR CREDIT
ICCL
B3
CCPs
Clearing members
Membership between clearing

Figure 8

Deloitte and Simudyne, two Cloudera partners, have extended this into the ABM framework. They have developed a cloud-enabled ABM simulation model of CCPs.[28] As illustrated in Figure 9, CCPs have clearing members which not only transact but are responsible for replenishing a default fund in case of clearing member defaults.

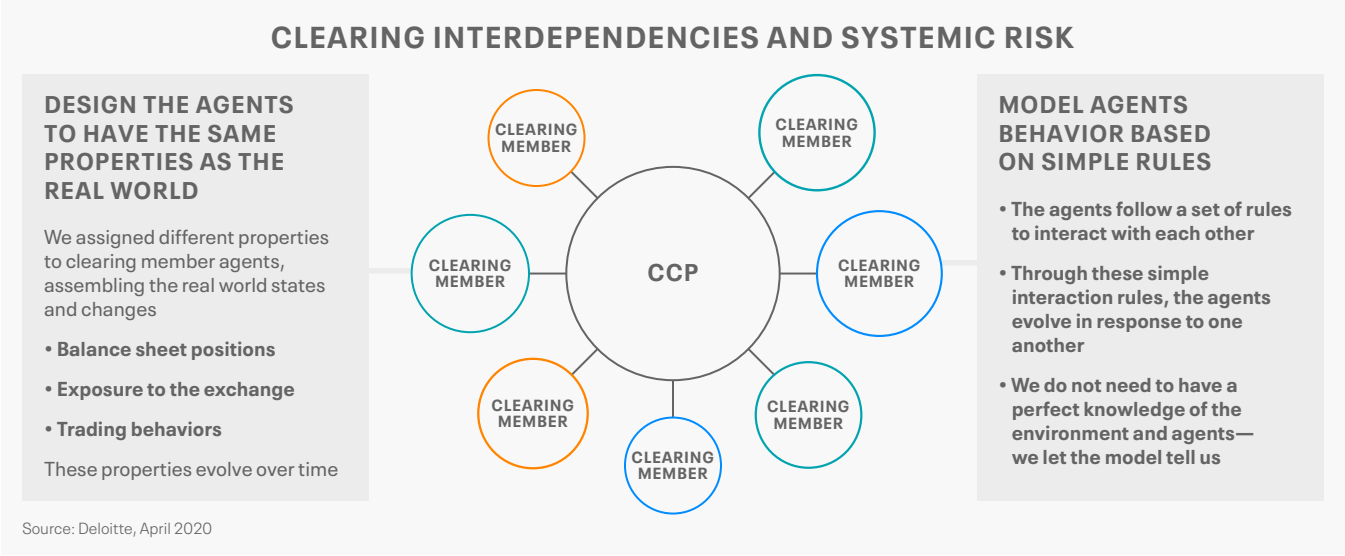

Figure 9

This model will be able to capture many of the risk exposures of CCPs (e.g., concentration risk, liquidity risk and wrong-way risk) which can have wide financial stability implications.

One can easily extend this type of ABM model to address specific Cloud Concentration Risk exposures with the capability for undertaking stressed analysis across thousands of scenarios. In the context of this paper, CCP related Cloud Concentration Risk is an important yet hidden dynamic that needs to be modelled, monitored and managed from a financial stability perspective—especially given the highly interconnected nature of CCPs, their clearing members and underlying CSP dependencies.

The Deloitte/Simudyne ABM modelling effort is a notable example for regulators and financial institutions to consider as a complementary approach to traditional approaches for quantifying potential future systemic risk events.

[28] Weston, Stephen and Zhang, Tiffany. "Agent-based modelling for central counterparty clearing risk: CCP Resilience—from One Crisis to the Next." Deloitte, April 2020.

Critical Need for a Cloud Migration Strategy and Cloud Transparency

As the entire Financial Services industry moves towards a hybrid, multi-cloud environment, an Enterprise Data Cloud framework enables institutions and regulators to more effectively gain the benefits of the cloud while also better managing cloud-related operational and systemic related risks.

Deloitte is a leader in advising banks on developing a comprehensive Cloud Strategy that considers regulatory oversight requirements. They have three Regional Centers for Regulatory Strategy with the EMEA center being led by David Strachan, formerly of the UK FSA. Their overall roadmap for developing a comprehensive Cloud strategy consists of the following phases:[29]

- Develop a more collaborative regulatory engagement at the outset
- Develop a clearly defined set of business objectives and related business case
- Develop the appropriate knowledge and skill sets from the board level to the IT staff
- Develop a comprehensive cloud governance framework
- Develop an integrated risk and control environment with clear allocation of ownership

Institutions following these guidelines will be more likely to accelerate and optimize their cloud migration journey while ensuring regulatory authorities are fully aware of their plans to become a more cloud-driven firm.

In addressing regulators' overall concerns around operational resilience, institutions must first specify the most important business functions that can impact financial stability risks. This requires a careful mapping of the systems, facilities, people, processes and third parties that support those business services. From this, institutions need to identify how the failure of an individual system or process running in the cloud environment could impact the operations of a specific business function and assess to what extent these systems or processes are capable of being substituted during disruption so that business services can continue to be delivered.

Only when this thorough mapping has been completed can the institution begin to assess the vulnerabilities and resulting concentration risk exposures that might result.

[29] Strachan, David. "Transitioning to the Cloud: considerations for firms." Deloitte Blog, September 16, 2019.

But this only addresses the operational risks that are specific to each institution. With the current high level of CSP vendor concentration, any disruptions of a key CSP has the potential under certain circumstances to trigger wider systemic impacts. For instance, the European Systemic Risk Board's (ESRB) systemic cyber risk study[30] provides a prominent type of incident effect whereby a "systemic cyber incident" could threaten financial stability. The key tipping point in these circumstances would occur when confidence in the financial system was so severely weakened that important financial institutions would cease all lending activity because they were no longer willing to lend, as opposed to being (technically) unable to lend. This is reflective of the Lehman Brother collapse on September 15, 2008 and the resulting impact across the wider financial system.

So How Should Regulators Address These Challenges?

The obvious first step in addressing Cloud Concentration Risk is the need for transparency in identifying the types of applications each institution currently has running as well as future applications planned for each CSP. Ideally, this would incorporate a standardized classification system for key financial infrastructure capabilities.

Collecting this data, permits regulators and industry participants to better identify potential contagion scenarios and trigger points that require regulatory oversight and possibly intervention. For example, one type of concentration risk that is of great concern arises if a significant number of institutions have a key application or market infrastructure capability (e.g., payment, settlement and clearing systems) concentrated in a single CSP.

This data centric approach enables regulators and industry participants to develop comprehensive dynamic stress tests. A further step would be to have institutions undertake coordinated reverse stress tests to bolster a regulator's ability to identify emerging systemic risk events.

[30] European Systemic Risk Board. "Systemic cyber risk", ESRB, February 2020.

References

1. Adrian, Merv. "Stop Talking About 'Hadoop'." Gartner Blog, March 4, 2020.
2. Ashlett, Matt. "Don't Call It A Comeback: Cloudera Accelerates It Hybrid Cloud Strategy." 451 Research, March 13, 2020.
3. Asia Cloud Computing Association (ACCA). "Asia's Financial Services on the Cloud 2018: Regulatory Landscape Impacting the Use of Cloud by Financial Services Institutions in Asia." ACCA, (2018)
4. Australian Prudential Regulatory Authority. "Outsourcing Involving Cloud Computing Services." APRA, Information Paper, September 24, 2018.
5. Bank of England. "How reliant are banks and insurers on cloud outsourcing?" Bank Overground, January 17, 2020.
6. Bank of International Settlements. "Regulating and supervising the clouds: emerging prudential approaches for insurance companies." FSI Insights on policy implementation, November 13, December, 2018.
7. Bank of England. "Bank of England's response to the van Steenis recommendations."
8. BoE, FCA and PRA. "Building the UK financial sector's operational resilience." Joint Discussion Paper, July 2018.
9. Bank of England. "How reliant are banks and insurers on cloud outsourcing?" Bank Overground, January 17, 2020.
10. Bank of International Settlements. "Regulating and supervising the clouds: emerging prudential approaches for insurance companies." FSI Insights on policy implementation, November 13, December, 2018.
11. Bank of England—Prudential Regulation "Outsourcing and third party risk management." Consultation Paper, CP30/19 (December, 2019)
12. Berg et al. "EBA Guidelines On Outsourcing Arrangements Have Entered Into Force." October, 2019.
13. BitSight. "Managing risk in an increasingly regulated world". BitSight White Paper. (2020)
14. Bookstaber, Richard, Paddrik, Mark and Tivanax, Brian. "An Agent-based Model for Financial Vulnerability." Journal of Economic Interaction and Coordination, 2018, vol. 13, issue 2, 433-466.
15. Central Bank of Ireland. "Outsourcing—Findings and Issues for Discussion." November 2018.
16. Cloudera. "Why a Successful Hybrid Cloud Strategy Requires an Enterprise Data Strategy: Five Strategic Considerations for Hybrid Cloud Success." Cloudera White Paper, January 2020.
17. Crisanto, J., Donaldson, C., Ocampo, D. and Prenio, J. "Regulating and supervising the clouds: emerging prudential approaches for insurance companies." BIS: FSI Insights, November 13, December 2018.
18. Dadoun, Dave. "Supporting modern technology policy for the financial services industry—guidelines by the European Banking Authority." Microsoft Perspectives, September 4, 2019.
19. Donnely, Caroline. "EBA outsourcing guidelines: What banks, fintechs and cloud providers need to know". Computer Weekly, September 19, 2019.
20. European Securities and Markets Authority. "ESMA Supervision—Annual Report 2019 and Work Programme 2020." ESMA 80-199-332, March 9, 2020.
21. European Banking Authority. "Final Report on EBA Guidelines on outsourcing arrangements." (EBA/GL/2019/02), February 25, 2019.
22. European Insurance and Occupation Pensions Authority. "Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers." EIOPA-BoS-19/270, July 1, 2019.
23. European Systemic Risk Board. "Systemic cyber risk", ESRB, February 2020.
24. FCA Finalised Guidance. "FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services." (Updated September 19, 2019)
25. Financial Stability Board. "Third-party dependencies in cloud services: Considerations on financial stability implications." FSB Publication, December 9, 2019.
26. Financial Stability Board. "FinTech and market structure in financial services: Market developments and potential financial stability implications." FSB Publication, February 14, 2019.
27. Gartner. "Forecast: Public Cloud Services, Worldwide, 2017-2023, 3Q19 Update." November 2019.
28. Gartner. "Cloud Data Ecosystems Emerge as the New Data and Analytics Battleground." January 29, 2020.

29. Hamilton, Alexander. "International regulators investigating tech firms' cloud dominance." FinTech Futures, October 3, 2019.
30. Harmon, Richard. "Cloud Concentration Risk: Will This Be Our Next Systemic Risk Event?" Cloudera White Paper, May 2018.
31. Majithia, Rakesh. "At A Glance: EBA issues revised guidelines on outsourcing." PWC, February 2019.
32. Pederson, Brendon. "Does Amazon-Google-Microsoft hold on the cloud pose a risk to banking?" American Banker, September 30, 2019.
33. Roland, Neil. "Tech giants' cloud services for banks under FSB scrutiny, Fed's Brainard says." mLex News, September 27, 2019.
34. Scalon, Luke. "MPs urge UK to consider regulation of cloud providers." Out-Law News, October 29, 2019.
35. Scott, Gulliver & Nadler. "Cloud Computing in the Financial Sector: A Global Perspective." Program on International Financial Systems, July, 2019.
36. Singapore: "Cyber panel flags concentration risk in cloud technology for banks, insurers." The Business Times, October 2, 2018.
37. Soramaki, Kimmo and Cook, Samantha. "Mapping clearing interdependencies and systemic risk." FIA, September 27, 2018.
38. Strachan, David. "Financial services on the Cloud: the regulatory approach." Deloitte Blog, 16/09/2019.
39. Strachan, David. "Regulatory barriers to the Cloud in financial services: perceived or real?" Deloitte Blog, 16/09/2019.
40. Strachan, David. "Transitioning to the Cloud: considerations for firms." Deloitte Blog, 16/09/2019.
41. UK House of Commons Treasury Committee. 'IT failures in the Financial Services Sector." Second Report of Session 2019-20, October 22, 2019.
42. Watts, Stephen and Raza, Muhammad. "SaaS vs PaaS vs IaaS: What's The Difference and How To Choose." BMC Blog, June 15, 2019.
43. Weston, Stephen and Zhang, Tiffany. "Agent-based modelling for central counterparty clearing risk: CCP Resilience—from One Crisis to the Next." Deloitte, April 2020.
44. WSBI-ESBG. "Cloud: Continued private-public dialogue needed to tackle challenges ahead." October 29, 2019.

About the Author

Dr. Harmon joined Cloudera in 2016 and is the Managing Director of Cloudera's Financial Services Industry vertical. He has over 25 years of experience in Capital Markets with specializations in Risk Management, Advanced Analytics, Fixed Income Research and Simulation Analysis. He started his career at the Federal Reserve Bank of New York followed by leading fixed income and mortgage research/quant teams at Citibank, Bankers Trust, JP Morgan and Bank of America/Countrywide Capital Markets. He was the co-founder of a GMAC funded Risk Management & Analytics start-up called Risk Monitors which was acquired by BlackRock, where he was a MD & Partner in the Risk Management Group. Dr. Harmon left Blackrock to start and manage the North American business for Norkom Technologies which was later sold to BAE systems. Starting in 2010, Richard was the Director of SAP's EMEA Capital Markets group for 6 years, where he helped grow the business across the EMEA region. Dr. Harmon holds a PhD in Economics with specialization in Econometrics from Georgetown University.

Contact: rharmon@cloudera.com

About Cloudera

At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world's largest enterprises.

CLOUDERA

Cloudera, Inc. 395 Page Mill Road Palo Alto, CA 94306 USA cloudera.com