PIFS

Program on International Financial Systems

Cloud Adoption in the Financial Sector and Concentration Risk

April 2023

The Program on International Financial Systems (PIFS) is a 501(c)(3) organization that conducts research on issues impacting the global financial system. PIFS also hosts international symposia, executive education programs and special events that foster dialogue and promote education on these issues. PIFS was founded in 1986, by Hal S. Scott, now Professor Emeritus of Harvard Law School. Over thirty years later, Hal Scott continues to lead PIFS.

This report was prepared by Hal Scott (Chairman and President of PIFS), John Gulliver, (Executive Director), Hillel Nadler (Senior Research Fellow), and Jon Ondrejko (Senior Vice President of Programs).

Amazon Web Services, Inc. is a financial sponsor of PIFS.

Cloud Adoption in the Financial Sector and Concentration Risk

APRIL 2023

Table of Contents

EXECUTIVE SUMMARY [1]

Cloud services have become an important part of the information technology toolkit in the global financial sector. As cloud adoption by financial institutions has increased, financial regulators have raised concerns about potential concentration risk resulting from cloud migration.[2] This report aims to provide clarity around the discussion of cloud adoption and concentration risk in the financial sector.

Section I of the report provides background on cloud adoption in the financial sector. Section II clarifies the potential risks associated with the use of third-party technology service providers by financial institutions, and examines those risks in the context of cloud adoption and traditional information technology (IT) infrastructure. Section III outlines the regulatory frameworks in different jurisdictions for addressing potential concentration risks associated with cloud adoption. Section IV concludes by setting out policy recommendations for mitigating potential concentration risks associated with cloud adoption in the financial sector.

The report has several key takeaways:

- Concentration risk is not new to the financial sector, nor is it unique to the cloud. Indeed, it is not obvious that such risks could be avoided if financial institutions were to rely on traditional IT infrastructure instead of the cloud. The critical question is how to manage or mitigate concentration risk.
- In order to assess the landscape of concentration risk in the financial sector, regulators should develop a clear and consistent definition of concentration risk and the underlying scenarios to which that definition applies.
- Regulators should also focus on gathering information about technology outsourcing by financial institutions, including the use of cloud-based services. Concentration risk can be addressed through information sharing and coordination among FIs, cloud providers, and supervisory authorities.
- Cloud adoption in the financial sector is still in its early stages. As cloud adoption increases, regulators should weigh the risks of concentration against the benefits of scale and quality of services provided by major cloud providers.
- In developing regulatory and supervisory approaches, regulators should engage directly with cloud providers in order to understand the tools available to financial institutions and the security and resiliency practice of cloud providers.
- Regulatory requirements and supervisory practices for cloud adoption should be tailored to specific risks and a one-size-fits-all approach should not be adopted for all financial institutions.

[1] PIFS would like to thank Andreas Dombret (Former Member of the Board of Deutsche Bundesbank), Bill Coen (Former Secretary General of the Basel Committee on Banking Supervision), David Chayer (Managing Director at The Depository Trust & Clearing Corporation), Richard Berner (Clinical Professor of Management Practice in the Department of Finance at New York University Stern School of Business), and Jon Danielsson (Director of the Systemic Risk Centre at the London School of Economics) for reviewing and providing comments on this report.

[2] *See* U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

PART I: CLOUD ADOPTION IN THE FINANCIAL SECTOR

Cloud services have become important IT building blocks for financial institutions globally. Before considering how cloud adoption affects concentration risk in the financial sector, this section provides necessary background on cloud adoption in the financial sector: it distinguishes between different types of cloud services, outlines the benefits and risks of cloud adoption, and describes the current state of cloud adoption by financial institutions.

a. Types of cloud services

Financial institutions (FIs) have historically relied on their own IT infrastructure, which was typically managed internally and by third-party technology companies.[3] To better manage increasing IT demands, such as those associated with digital delivery channels including mobile and internet services, FIs are transitioning from this on-premises IT infrastructure model to the use of cloud-based services offered by individual cloud service providers to many different customers at scale.[4]

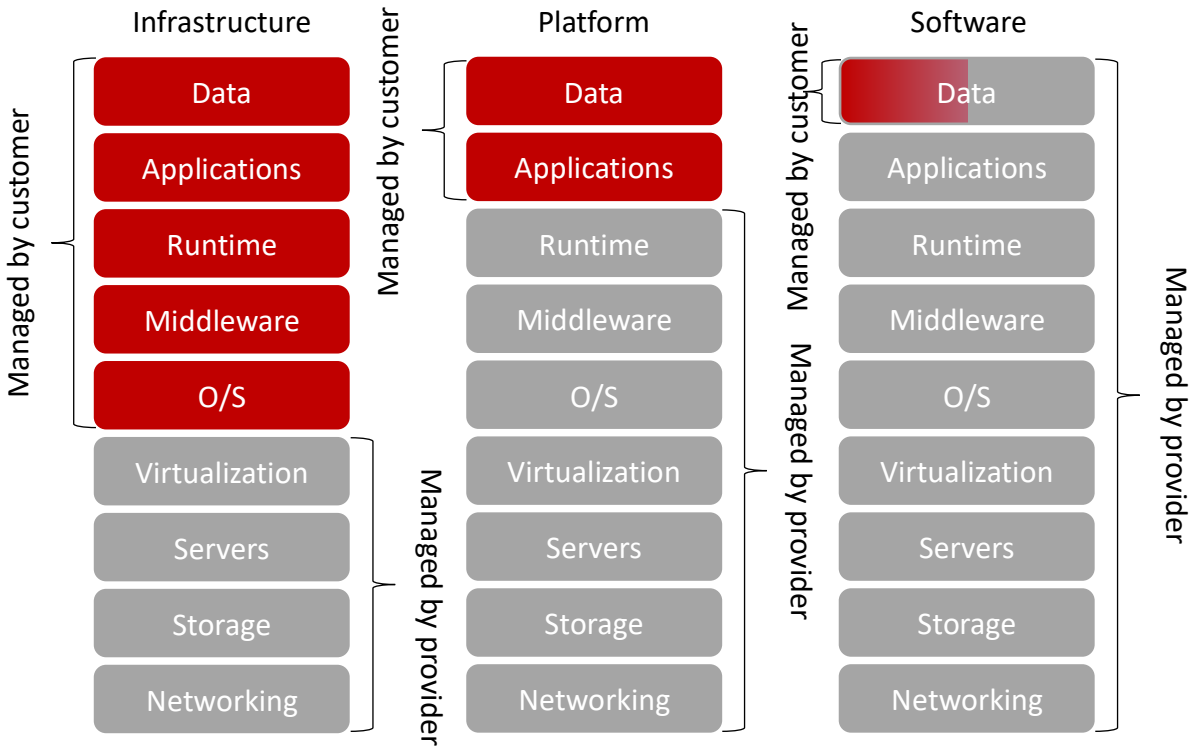
Cloud computing can refer to any use of computing resources over a network, such as the internet, in a manner that is scalable with demand.[5] Cloud-based services can be divided into three basic types, based on the nature of computing resources that the customer uses: infrastructure, platform, and software services.

When a FI uses computational *infrastructure*, such as servers, storage capacity or networking, cloud providers control the underlying infrastructure and orchestration while the FI defines and manages a significant part of the virtual infrastructure using these services, including the operating systems and the applications that run on that infrastructure. At the other end of the spectrum, FIs can run *software* developed and controlled by a cloud service provider on remote servers. A FI can also use *platform* services to develop and use software on hosting and development infrastructure offered by a cloud service provider. Platform services offer more structure than more bare-bones infrastructure services but more flexibility than provider-developed and -controlled software services.[6] **Figure 1** illustrates the three types of cloud-based services.

---

[3] Filip Blazheski, Cloud banking or banking in the clouds?, BBVA Research 1 (BBVA Research, April 29, 2016), available at https://www.bbvaresearch.com/wp-content/uploads/2016/04/Cloud_Banking_or_Banking_in_the_Clouds1.pdf.
[4] W. Kuan Hon & Christopher Millard, Cloud Computing vs. Traditional Outsourcing – Key Differences, 23 Computers & Law 4 (Oct./Nov. 2012), https://ssrn.com/abstract=2200592.
[5] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, 2 (NIST Special Publication 800-145, Sep. 2011), available at https://doi.org/10.6028/NIST.SP.800-145.
[6] Eric Simmon, *Evaluation of Cloud Computing Services Based on NIST SP 800-145*, 8-11 (NIST Special Publication 500-322, Feb. 2018), available at https://doi.org/10.6028/NIST.SP.500-322. This report focuses primarily on "public" cloud, which involves the use of standardized, commoditized cloud-based services by multiple different customers. Unlike public cloud, "private" cloud typically refers to computing resources that are dedicated by a cloud service provider to a single customer. So-called "hybrid" cloud solutions involve the mixed use of private and public cloud, for example, the use of private cloud for storage and processing of particularly sensitive information but public cloud for other information. Id at 12-17. Major cloud providers also offer "virtual" private clouds, which share physical infrastructure with a public cloud but are logically isolated from the rest of the cloud. See, for example, Amazon Web Services, *Amazon Virtual Private Cloud: User Guide* 1- 8 (2022), available at https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf.

Figure 1



These different types of cloud services can be layered on top of each other. For example, fintech startups that offer cloud-based software services often build those services using the infrastructure or platform services of a major cloud provider, rather than using their own computing infrastructure.[7]

An FI's choice of cloud services is shaped by its needs, technical capabilities and staff knowledge and skill. For example, FIs with more in-house technical expertise, whether large banks or small fintech startups, may use infrastructure resources to build entirely new applications. FIs with less technical expertise may choose to use the cloud to run software developed by third-party solutions providers, which is easier to deploy and operate.

b. Factors shaping the cloud adoption decision

The decision to move from traditional on-premises IT infrastructure to the cloud is often driven by the lower costs and increased efficiency of cloud services. Cloud services are also more agile than traditional IT infrastructure, an aspect highlighted by the COVID-19 pandemic. Still, FIs must evaluate potential technological and operational challenges when considering cloud adoption.

[7] W. Kuan Hon and Christopher Millard, *Banking in the cloud: Part 1 – banks' use of cloud services*, 34 Computer Law & Sec. Rev. 4, 6 (2018).

Reasons for cloud adoption

To ensure their smooth operation on traditional on-premises IT infrastructure, FIs often need to maintain IT resources (plus the skilled human resources necessary to manage them) at a level that exceeds their everyday needs. This excess computing and human capacity is necessary to support FIs' highest projected volume requirements, even if that capacity is rarely used.[8] Cloud technology can minimize the need for this kind of costly over-provisioning by allowing FIs to benefit from the economies of scale inherent in sharing a cloud provider's computing resources and technical support across its many customers. FIs can quickly scale up in an automated manner when additional resources are needed and scale down when demand subsides.[9]

By making computing resources and technical support available on demand to customers who pay only for what they actually use, the cloud turns large, up-front capital expenditures into variable operational costs that depend on actual usage.[10] For FIs, this translates to lower costs for purchasing, support and maintenance of IT infrastructure. It also makes FIs more technologically agile: they can test new scenarios, software tools and alternative configurations without a lengthy purchasing and provisioning process.[11] Deploying a server on the cloud can take as little as a few minutes, as opposed to the up to nine weeks it can take to deploy a server in a traditional proprietary data center.[12]

The increased agility made possible by cloud services was on display during the Covid-19 pandemic. The pandemic caused an abrupt transition to a remote workplace environment for corporate employees. FIs were forced to rapidly expand their reliance on cloud-based services, especially collaboration tools, to support their remote workforce.[13] The onset of the pandemic also forced FIs to offer remote services to clients, instead of in-person options like bank branches. Many FIs used cloud-based tools like virtual desktops to maintain service levels in a remote environment.[14]

Other factors affecting cloud adoption

Other considerations have also affected cloud adoption in the financial sector. Some of these considerations are institutional: generally, FIs tend to be largely conservative organizations and can therefore be reluctant to deploy new technologies.[15] Deployment-

[8] Depository Trust & Clearing Corporation (DTCC), *Moving Financial Market Infrastructure to the Cloud*, 5-6 (2017).
[9] Id at 6; Blazheski, *Cloud banking or banking in the clouds?*, 1.
[10] DTCC, *Moving Financial Market Infrastructure to the Cloud*, 6; Douglas Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals*, 8 (Microsoft, 2017), https://download.microsoft.com/download/0/D/6/0D68AE95-6414-4074-B4B8-34039831E2BF/Introduction-to-Cloud-Computing-for-Legal-and-Compliance-Professionals.pdf.
[11] Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services*, 7.
[12] Barb Darrow, *Why Fortune 500 Companies Are Trusting the Cloud More Than Ever*, Fortune (Sep. 13, 2017), http://fortune.com/2017/09/13/amazon-microsoft-google-sap-cloud/.
[13] Lananh Nguyen, *Banks Tiptoe Toward Their Cloud-Based Future*, New York Times (Jan. 3, 2022), https://www.nytimes.com/2022/01/03/business/wall-street-cloud-computing.html; Jerry Silva and Karen Augustine, *Banking on the Cloud: Results from the 2021 CloudPath Survey*, 6 (IDC Perspective, August 2021).
[14] Daniel Pujazon and Brad Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, 4-5 (Institute of International Finance, June 2020).
[15] Nguyen, *Banks Tiptoe Toward Their Cloud-Based Future*.

related challenges are another factor in impeding cloud adoption; FIs can have difficulty integrating their legacy infrastructure with newer cloud resources. As a result, many FIs initiate their cloud adoption with newer or novel workloads and applications, rather than moving older legacy applications to the cloud.[16]

Regulatory considerations also factor into financial firms' decisions regarding cloud adoption. As described in Part III, while some financial regulations and guidance have been updated—or are in the process of being updated-to explicitly address cloud adoption, regulatory uncertainty persists.[17] In addition, for FIs that operate across different jurisdictions, inconsistent cross-border requirements and data localization restrictions can limit the benefits of cloud adoption by making it more difficult to leverage the distributed nature of cloud services and enable greater operational resilience.[18]

c. Benefits and risks of cloud adoption by financial institutions

In addition to the efficiency and agility benefits that are driving the shift to cloud services, FIs that have made the move to the cloud find that it offers additional benefits.[19] Cloud adoption also offers potential benefits for the broader financial sector. At the same time, cloud adoption also gives rise to potential risks.

Benefits of cloud adoption

Cloud services can be more secure than traditional IT platforms.[20] While some FIs—especially larger, more sophisticated ones—are able to devote significant financial and personnel resources to security, smaller FIs may not. The major cloud providers, by contrast, tend to be at the forefront of security research and implementation, enabling the faster discovery and mitigation of security vulnerabilities, which benefits FI customers of all sizes.[21] Major cloud providers' infrastructures are also generally built to support stringent security requirements and protocols—although it is ultimately up to individual FIs to make use of those tools.[22]

Since the cloud infrastructure of major cloud providers is widely distributed, with hundreds of data centers located across the globe, the cloud can also enable greater resiliency in the financial sector.[23] FIs can distribute processes and data across a cloud provider's different data centers, allowing them to build applications that can be online even if a

[16] Pujazon and Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, 6-7; Jerry Silva, *Banking on the Cloud: Results from the 2020 CloudPath Survey*, 7-8 (IDC Perspective, Nov. 2020).
[17] Pujazon and Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, 6.
[18] Id.
[19] Silva and Augustine, *Banking on the Cloud: Results from the 2021 CloudPath Survey*, 6-8 (describing separately reported triggers for cloud adoption and reported benefits of cloud adoption).
[20] Blazheski, *Cloud banking or banking in the clouds?*, 5; DTCC, *Moving Financial Market Infrastructure to the Cloud*, 7.
[21] The major cloud providers, for example, quickly mitigated significant chip-level security vulnerabilities that had been discovered by one of the providers. Jordan Novet, *Amazon, Microsoft, and Google respond to Intel chip vulnerability*, CNBC (Jan. 3, 2018) https://www.cnbc.com/2018/01/03/microsoft-google-respond-to-intel-chip-vulnerability.html.
[22] Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services,* 8; DTCC, *Moving Financial Market Infrastructure to the Cloud*, 6.
[23] Id.

particular data center or region experiences a disruption.[24] Likewise, the scalability of cloud services allows FIs to handle unexpected capacity requirements, whether due to an unanticipated surge in trading activity or a malicious cyberattack, in ways that they would not otherwise be able to if relying solely on their own IT infrastructure.[25]

Another benefit of the increased computing resources and scalability of the cloud is the ability to build analytic tools that can be leveraged by FIs and regulators to better understand and manage operational risks in the financial system.[26] In addition, the cloud can benefit the financial sector by creating a more level playing field between FIs of different sizes. The lower up-front costs of cloud services allow small- and medium-sized FIs, as well as fintech startups, access to computing resources that previously would have been available only to larger FIs.[27]

Risks related to cloud adoption

Many of the risks related to cloud adoption are also associated with traditional IT infrastructure. The use of cloud services, for example, does not entirely eliminate the need for capacity planning with respect to computing resources. It just delegates the underlying infrastructure-related capacity planning decisions to cloud providers, who must predict aggregated demand for resources across all of their customers to meet their needs.[28]

Nor does cloud adoption eliminate the potential for unauthorized access to an FI's data or processes. Most cloud service providers run on a shared responsibility model. The cloud service provider leaves certain customer environment specific configurations to the customers that, if poorly managed, can lead to security risks. In a cloud environment, customers remain at risk, for example, of overly permissive access controls or mismanagement of encryption keys. These risk would exist whether these credentials were stored on-premises or in the cloud.[29]

Multi-tenancy—the ability of multiple customers to share the same infrastructure—is a critical feature of cloud services. However, it is not unique to the cloud; it has existed in hosted applications and other traditional IT configurations that predate cloud computing. Some cybersecurity analysts have raised concerns that customers using shared infrastructure resources in the cloud might expose their data or processes to unauthorized

---

[24] Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals,* 10.
[25] Amazon Web Services, *AWS Best Practices for DDoS Resiliency*, 6-15 (Dec. 2018), https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf.
[26] Paul J. Davies, *New Tools Give Better Picture, Literally, of Financial-System Risk*, Wall Street Journal (April 24, 2017), https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk-1493086260?mod=article_inline; Basel Committee on Banking Supervision, *Sound Practices: Implications of fintech developments for banks and bank supervisors*, 24 (Feb. 2018), https://www.bis.org/bcbs/publ/d431.pdf.
[27] World Bank Group and International Monetary Fund, *Bali Fintech Agenda – Chapeau Paper* 17 (Sep. 19, 2018), http://documents.worldbank.org/curated/en/390701539097118625/pdf/130563-BR-PUBLIC-on-10-11-18-2-30-AM-BFA-2018-Sep-Bali-Fintech-Agenda-Board-Paper.pdf.
[28] Tom Krazit, *How Amazon Web Services uses machine learning to make capacity planning decisions*, GeekWire (May 18, 2017), https://www.geekwire.com/2017/amazon-web-services-uses-machine-learning-make-capacity-planning-decisions/.
[29] Ramaswamy Chandramouli, Michaela Iorga and Santosh Chokhani, *Cryptographic Key Management Issues & Challenges in Cloud Services*, National Institute of Standards and Technology Interagency or Internal Report 7956 (Sep. 2013), http://dx.doi.org/10.6028/NIST.IR.7956.

parties.[30] Such exposure may result from the exploitation of vulnerabilities associated with the hypervisor (the software program which manages the virtual machines that make up the cloud).[31]. However, such risks may be mitigated in the cloud through the use of a dedicated host (a physical server that is dedicated for a customer use) instead of multi-tenant servers.

The relationship between FIs and their cloud service providers can result in operational risks, which are also similar to those that arise in connection with traditional IT outsourcing. In any relationship with a third-party vendor, FIs must manage the risks associated with subcontracting by the vendor.[32] Likewise, in any relationship with an IT service provider, FIs can be exposed to a degree of "lock-in" risk. Lock-in can arise out of an FI's legal obligations, for example, where its agreement with a cloud services provider includes exclusivity terms. Even in the absence of any such exclusivity requirements, an FI can become excessively dependent on a particular service provider.[33]

The on-demand nature and scale of cloud services allows them to be provided to more customers in a more automated manner than traditional technology platforms, potentially increasing the concentration of FIs using a particular cloud provider. Reliance by FIs on a small number of cloud providers or services could theoretically result in the emergence of new dependencies at both the firm level and in the financial system as a whole.[34] The risks arising out of these potential dependencies, are addressed in more detail in Part III.

d. The current state of cloud adoption in the financial sector

The move toward cloud services in the financial sector was already well underway prior to the onset of the COVID-19 pandemic. According to one industry survey, as of 2021 more than 90 percent of responding banks had adopted cloud for at least some workloads.[35] Another survey, taken during the first months of the pandemic, reported that a third of all IT spending at banks was allocated to public cloud, up from less than 20 percent in 2018.[36] As noted above, the pandemic accelerated the demand for cloud services in the financial sector.[37]

---

[30] Timothy Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, Carnegie Mellon University Software Engineering Institute (March 5, 2018), https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html/.

[31] Donald Firesmith, *Multicore and Virtualization: An Introduction*, Carnegie Mellon University Software Engineering Institute (Aug. 14, 2017), https://insights.sei.cmu.edu/sei_blog/2017/08/multicore-and-virtualization-an-introduction.html; Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*.

[32] Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*.

[33] Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services*, 11-12; Justice Opara-Martins, Reza Sahandi and Feng Tian, *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, Journal of Cloud Computing: Advances, Systems and Applications (2016), https://journalofcloudcomputing.springeropen.com/track/pdf/10.1186/s13677-016-0054-z; Jérôme Barthélemy, *The Hidden Costs of IT Outsourcing*, MIT Sloan Management Review (April 2001), https://sloanreview.mit.edu/article/the-hidden-costs-of-it-outsourcing/.

[34] Financial Stability Board (FSB), *FinTech and market structure in financial services: Market developments and potential financial stability implications*, 17 (Feb. 14, 2019), http://www.fsb.org/wp-content/uploads/P140219.pdf

[35] American Bankers Association, Cloud Computing in the U.S. Banking Industry (June 2021).

[36] Silva, *Banking on the Cloud: Results from the 2020 CloudPath Survey*, 3-4.

[37] Nguyen, *Banks Tiptoe Toward Their Cloud-Based Future*; Silva and Augustine, *Banking on the Cloud: Results from the 2021 CloudPath Survey*, 6; Pujazon and Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, 4-5.

Nevertheless, cloud adoption in the financial sector is varied and, for many FIs, still in its early stages. Some FIs have retired their on-premises IT architecture and gone "all-in" on cloud adoption. Other FIs have moved certain operations, especially enterprise applications such as human resources and collaboration tools, to the cloud. However, critical operations—those involved in processing transactions, updating accounts, and reconciling ledgers—are still largely conducted using legacy IT systems.[38] A post-pandemic survey of over 100 global banks reported that North American banks had migrated just 12 percent—and European banks just five percent—of their total workloads to the cloud. For "core" workloads—defined as workloads related to core systems, such as back-end process and systems that manage customer interactions throughout the bank—the percentage of workloads that had been migrated to the cloud by the responding banks stood at a paltry three percent.[39]

PART II: CLOUD ADOPTION AND "CONCENTRATION RISK"

As the use of cloud services in the financial sector becomes more prevalent, financial regulators and other policymakers, including the U.S. Treasury Department in its recently released report on cloud adoption in the financial sector, have raised concern about potential "concentration risks".[40] This section aims to clarify the potential concentration risks associated with FIs' use of third-party technology service providers. It then considers those risks in the context of cloud adoption and compares them to concentration risks associated with traditional IT infrastructure. Finally, this section concludes with a discussion of the measures that FIs and cloud providers already take to mitigate concentration risks associated with cloud adoption.

a. Concentration risk in the financial sector

Although there is no agreed-upon definition of concentration risk, it can be thought of as including any "probability of loss arising from a lack of diversification."[41] As a result, there is no single source of concentration risk in connection with the use of technology service providers. Rather, the lack of diversification that results from technology outsourcing can arise in a number of different ways and at several different levels. These different types of concentration risk are outlined below.

---

[38] Paul Tierno, *Bank Use of Cloud Technology*, 1 (Congressional Research Service, Dec. 2021), https://sgp.fas.org/crs/misc/IF11985.pdf.

[39] Accenture, *Banking Cloud Altimeter: Volume 1*, https://bankingblog.accenture.com/banking-cloud-altimeter-magazine/volume-1-what-does-banking-cloud-mean.

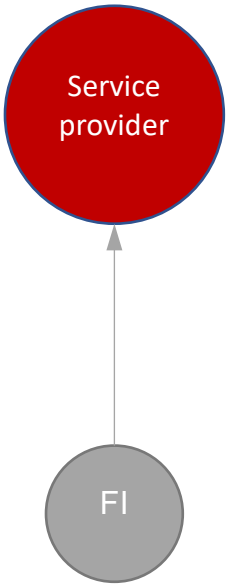
[40] Andew Duehren, *Treasury Says Cloud Computing Poses Risks to Financial Sector*, Wall St. J. (Feb. 8, 2023), https://www.wsj.com/articles/treasury-warns-of-risks-to-financial-sector-in-cloud-computing-services-11675823799; Iain Withers & Huw Jones, *For bank regulators, tech giants are now too big to fail*, Reuters (Aug. 20, 2021), https://www.reuters.com/article/finance-bigtech-idCNL4N2PH33Z.

[41] *BITS Guide to Concentration Risk in Outsourcing Relationships*, BITS: Financial Services Roundtable (2010), https://web.actuaries.ie/sites/default/files/erm-resources/bitsconcentrationrisk0910.pdf.

FI-specific concentration risk

Concentration risk can potentially arise at the "micro" level—at the level of an individual institution—if an FI becomes so dependent on a particular infrastructure or technology service provider that a disruption affecting that infrastructure or provider impairs the FI's ongoing functioning (see **Figure 2)**. This risk is exacerbated by "vendor lock-in", where an FI must rely on an individual provider, even in the event of failure, because it has no reasonable alternatives or substitute.[42]

Figure 2. FI-specific concentration risk.



Although it arises at the level of an individual FI, this kind of concentration risk can have consequences for the broader financial system. The financial system depends on a few key institutions and utilities.[43] If one of those institutions or utilities becomes dependent on a particular vendor, a disruption that affects the availability or integrity of that provider could have negative consequences for the financial system.[44]

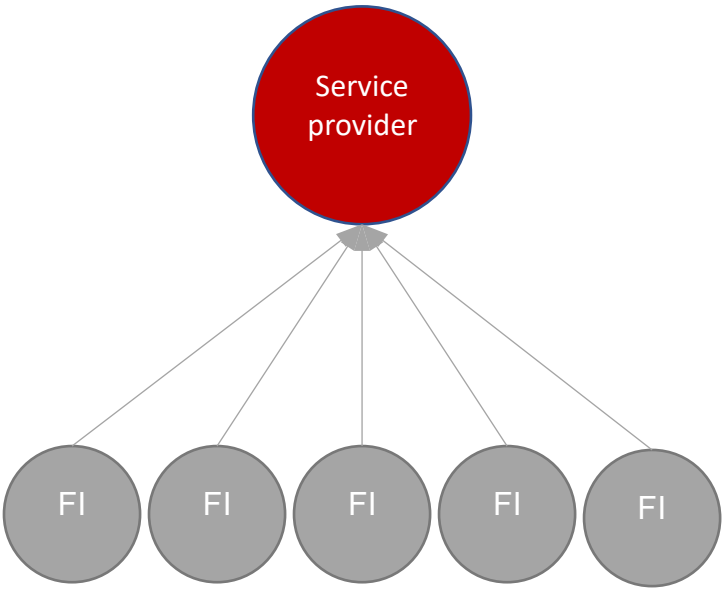
Systemic concentration risk

Another type of concentration risk—"macro" concentration risk—could theoretically arise in connection with the use by many FIs of the same third-party technology service provider (see **Figure 3**). In this situation, the failure of that service provider may adversely impact a significant portion of the financial sector. That failure could result from a major technological disruption—for example, if a disruption at one technology service provider

[42] Harmon, R. , Vytelingum P., and Babaie-Harmon, J., *Cloud Concentration Risk: A Framework Agent Based Model For Systemic Risk Analysis*, Journal of Financial Compliance (Spring 2021).
[43] These utilities include those responsible for such critical functions as securities custody, payment processing, collateral management, trade matching and confirmation, and clearing. See, e.g., Board of Governors of the Federal Reserve System, *Designated Financial Market Utilities*, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.
[44] See Section II.B.

simultaneously affects data or systems at many FIs. It could also result from a large-scale non-technological disruption at the service provider, such as financial distress.

Figure 3. Systemic concentration risk.



Concentration risk without a single provider

Industry-wide concentration risk may also result when multiple FIs adopt similar technological models, leaving them vulnerable to similar disruptions even if they do not all use the same provider. From approximately 2014 to 2018, for example, state-sponsored hackers embarked on a campaign of cyber theft from dozens of companies, including large FIs. They were able to compromise these companies by targeting their "managed service providers": third-party providers that are responsible for the remote management of their customers' IT infrastructure and the overlaying applications and tools.[45] Notably, not all of the affected companies used the same managed service provider. Rather the hackers gained access to *several* of these providers' systems by sending phishing emails that delivered malware to the providers, which then infiltrated their clients' networks.[46]

Moreover, the nature of concentration risk that results from technology outsourcing will be contextual, depending on factors such as the jurisdiction in which FIs and their service providers are located. FIs in one jurisdiction may face concentration risk in connection with their reliance on technology service providers in another jurisdiction—even if they do not depend exclusively on a single service provider in that jurisdiction. They may face the

[45] Gartner, Managed Service Provider (MSP) (last accessed April 2023), https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider
[46] "Operation Cloud Hopper," PwC and BAE Systems, April 2017, https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf.

possibility, for example, that authorities in the service providers' jurisdiction may sanction or restrict the provision of services to clients in their own jurisdiction.[47]

b. To what extent are concentration risks systemic?

Another important question is whether and how the concentration risks described above affect the financial system as a whole. The financial system has proven operationally resilient: disruptions resulting from the failure of a technology service provider can occur, even at great financial cost, without triggering a systemic crisis. In 2022, for example, a major outage shut down the business and consumer network services provided by a leading Canadian telecommunications company for almost an entire day.[48] The outage, which cost the Canadian economy an estimated $142 million across all sectors, shut down ATMs and electronic payment services for several large banks.[49] Once the outage was resolved, those banks suffered no lasting impact.

The potential impact of technological failure on the financial system

Historically, financial crises have been triggered by short-term creditors withdrawing their money from the financial system simultaneously, leading to a loss of liquidity and even failure of certain FIs.[50] These short-term creditors are typically motivated by a loss of confidence in the solvency or liquidity of one or more FIs. Specifically, they fear that will not obtain the full value of their deposit unless they immediately withdraw from the FIs. The disruption of an FI's data or systems would only contribute to such a run if it raised doubts about its underlying financial health or stability.[51]

How would the impact of technological failure change because of increased concentration risk?

In theory, concentration risk could increase the likelihood that a technological or operational failure has a systemic impact to an FI. The failure of a third-party provider could impair an FI's operations, leaving it unable to meet its payment obligations. [52] For example, the failure in 2012 of batch scheduling software at UK's NatWest RBS banking group disrupted many of its basic banking operations, leaving millions of customers unable to

[47] See, e.g., Francesco Guarascio, EU working on possible ban on providing cloud services to Russia – source, Reuters (June 8, 2022), https://www.reuters.com/technology/eu-working-possible-ban-providing-cloud-services-russia-source-2022-06-08/.

[48] CNBC, Rogers network outage across Canada hit banks, businesses and consumers (July 8, 2022), https://www.cnbc.com/2022/07/08/rogers-network-outage-across-canada-hit-banks-businesses-and-consumers.html

[49] See Michelle Zadikian and Iva Poshnjari, Rogers pledges five-day credits as Bay Street weighs outage impact, BNN Bloomberg (July 12, 2022), https://www.bnnbloomberg.ca/rogers-outage-could-cost-canada-s-economy-142m-analyst-1.1790982; Finextra, Rogers outage shuts down Canadian banks' ATMs, POS and internet banking (July 8, 2022), https://www.finextra.com/newsarticle/40611/rogers-outage-shuts-down-canadian-banks-atms-pos-and-internet-banking

[50] Diamond, D. W. & P. H. Dybvig, *Bank runs, deposit insurance, and liquidity*, Journal of Political Economy 91(3), 401–419 (1983) (panic-based runs); Goldstein, I. & A. Pauzner, *Demand–deposit contracts and the probability of bank runs*. Journal of Finance 60(3), 1293–1327 (2005) (fundamentals-based runs).

[51] Jon Danielsson & Robert Macrae, *Systemic consequences of outsourcing to the cloud*, VoxEU/CEPR (Dec. 2, 2019), https://cepr.org/voxeu/columns/systemic-consequences-outsourcing-cloud.

[52] Thomas M. Eisenbach, Anna Kovner, & Michael Junho Lee, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, Federal Reserve Bank of New York Staff Reports, no. 909, (May 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf.

access their accounts for several days.[53] The failure of a bank to meet its payment obligations could potentially lead to liquidity scarcity in the financial system.[54] Importantly, however, a failure of this sort will not necessarily have broader consequences to the financial sector: the NatWest outage was resolved without any larger systemwide fallout.

The systemic risk posed by technological failure is potentially greater if multiple FIs rely on a single technology service provider.[55] A failure at that provider might impair multiple FIs simultaneously, which under certain condition could cause a broader impact to the financial system. For example, the Federal Reserve suffered a widespread disruption in multiple payment services in February 2021, which included the Fedwire system that FIs rely on to transfer trillions of dollars each day. The disruption, which was attributed to operational error, lasted for several hours.[56] Again, however, the disruption did not have any long-term systemic consequences.

c. Concentration risks and cloud adoption

The cloud's model, which leverages the economies of scale associated with sharing computing resources, may also result in many FIs depending on a small number of providers.[57] According to a Bank of England survey, for instance, most banks and insurers rely on just two providers for cloud-based infrastructure services.[58] A disruption that compromises the security of data at a cloud-based service provider, or impairs the availability or integrity of data or systems at a cloud provider, could in theory affect the operations of many FIs at the same time. Periodic disruptions at major cloud providers, for example, have temporarily disrupted the operations of their clients, including FIs.[59] In December 2021, a service disruption at a major cloud provider caused widespread but transient disruptions at many (mostly non-financial) companies.[60]

Another potential source of concentration risk in the cloud relates to certain common linchpin technologies on which cloud deployments rely. These technologies are critical

---

[53] Tim Worstall, RBS/NatWest Computer Failure: Fully Explained, Forbes (Jun 25, 2012), https://www.forbes.com/sites/timworstall/2012/06/25/rbsnatwest-computer-failure-fully-explained/?sh=9ae3e0167c7f)

[54] Thomas M. Eisenbach, Anna Kovner, Michael Junho Lee, Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis. Federal Reserve Bank of New York (May 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf.

[55] Bank of England, DP3/22 – Operational resilience: Critical third parties to the UK financial sector, PRA Discussion Paper 3/22 | FCA Discussion Paper 22/3 (July 21, 2022), https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector

[56] Matt Egan, The Federal Reserve suffers widespread disruption to payment services, CNN Business (Feb. 25, 2021), https://www.cnn.com/2021/02/24/business/federal-reserve-outage-fedwire/index.html

[57] Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo & Jermy Prenio, *Regulating and supervising the clouds: emerging prudential approaches for insurances companies*, FSI Insights on policy implementation No. 13, 4 (Dec. 2018), https://www.bis.org/fsi/publ/insights13.pdf.

[58] Bank of England, How reliant are banks and insurers on cloud outsourcing? (Jan. 17, 2020), https://www.bankofengland.co.uk/bank-overground/2020/how-reliant-are-banks-and-insurers-on-cloud-outsourcing; Sophia Furber, As 'big tech' dominates cloud use for banks, regulators may need to get tougher, S&P Global (Aug. 18, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/as-big-tech-dominates-cloud-use-for-banks-regulators-may-need-to-get-tougher-59669007 (discussing the results).

[59] Tianjiu Zuo, Commercial Cloud Outages Are a Wake-Up Call, NextGov (March 17, 2021), https://www.nextgov.com/ideas/2021/03/commercial-cloud-outages-are-wake-call/172731/.

[60] Amazon Web Services, Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region (Dec. 10, 2021) https://aws.amazon.com/message/12721/.

systems, like routing, identity access management and virtualization, that support the secure and continued operation of the cloud network. The failure or disruption of a linchpin technology can have significant consequences for cloud providers and the users that depend on them.[61] In March 2021, a failed update to an authentication system relying on an identity and access management (IAM) component caused a nearly global outage at a major cloud provider.[62]

Concentration risk – not unique to cloud

As the prior discussion illustrates, however, technology or operational failures—even those that arise in connection with dependency on particular technological infrastructure or an individual service provider—are not new to the financial system. Lock-in risk, for example, is not unique to the cloud. FIs that contract with third-party service providers to build and maintain on-premises data centers, for instance, tend to enter into long-term contracts that can make switching providers difficult and economically costly. And a failure at an FI's managed, on-premises databases can knock out critical systems, like payments and other transactions.[63]

Likewise, the reliance of many FIs on common technologies is not a novel feature of cloud adoption. Even when using traditional, bespoke IT infrastructures, FIs have historically become reliant on common products and services, ranging from semiconductors to software to managed databases, that were produced or provided by a small number of third-party providers.[64] A vulnerability associated with one of these common products and services can give rise to the same sort of concentration risk that characterizes the common use of a cloud provider.

Moreover, while cloud adoption may give rise to concentration risks, it is not necessarily the case that such risks could be avoided if FIs were to rely or continue to rely on traditional IT infrastructure instead. The demands of FIs' customers and employees place increased emphasis on interconnectivity as a defining feature of their technology infrastructure. As FIs provide more internet and mobile access to external clients, as well as more flexibility for their internal workforce, they will become increasingly reliant on tools that manage that interconnectivity, whether they use on-premises or cloud infrastructure. The use of common product and services to manage the technological interconnectivity can

---

[61] Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo, Broken trust: Lessons from Sunburst, Atlantic Council (March 29, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/

[62] Caroline Donnelly, Microsoft cloud users hit by global outage linked to Azure Active Directory issue (March 16, 2021), https://www.computerweekly.com/news/252497921/Microsoft-cloud-users-hit-by-global-outage-linked-to-Azure-Active-Directory-issue

[63] FinExtra, IBM employee fingered as culprit in massive DBS outage (July 14, 2010), https://www.finextra.com/newsarticle/21603/ibm-employee-fingered-as-culprit-in-massive-dbs-outage (outage after IT failure); FinExtra, Singapore central bank slams DBS and IBM over systems outage (Aug. 5, 2010), https://www.finextra.com/newsarticle/21672/singapore-central-bank-slams-dbs-and-ibm-over-systems-outage (bank faulted for failure to diversify outsourcing risks).

[64] *BITS Guide to Concentration Risk in Outsourcing Relationships*, BITS: Financial Services Roundtable (2010), https://web.actuaries.ie/sites/default/files/erm-resources/bitsconcentrationrisk0910.pdf. See also Ben Thompson, Microsoft's Monopoly Hangover, Stratechery (July 26, 2017) https://stratechery.com/2017/microsofts-monopoly-hangover/ (describing historic dominance of IT providers).

add to concentration risk. Thus, the critical question is not how to eliminate concentration risk, but how to manage or mitigate it.

d. How do financial institutions and cloud providers mitigate concentration risk?

FIs and cloud providers currently take several measures to mitigate concentration risk that arises in connection with cloud adoption. This subsection outlines different steps that cloud providers and FIs can and do take to limit their exposure to concentration risk. In order to understand the different measures that can be taken by FIs and cloud providers to mitigate concentration risk, it is important to first explain the "shared responsibility" model developed by cloud providers to allocate responsibility for different aspects of cloud security and resiliency.

The "shared responsibility" model

Generally, large cloud providers rely on a "shared responsibility" model of cloud security and resiliency that defines the responsibilities of cloud providers and their customers for various aspects of the cloud environment.[65] Although the particular shared responsibility models formulated by the major cloud providers have some differences,[66] they share the same basic approach: cloud providers are responsible for the security and resiliency of the tools that they build (security and resiliency "of" the cloud), while users are responsible for how they use those tools (security and resiliency "in" the cloud).[67]

In practice, that means that cloud providers operate, manage and control the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The FI customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the environment and security.[68] The shared responsibility model enables FIs to decide where they put their data, as a way to mitigate determining their own political or regulatory or risk. This shared responsibility model for the IT environment also extends to IT controls and security.[69]

Under the shared responsibility model, cloud providers and users never share responsibility for the *same* aspect of cloud security or resiliency. A user's areas of responsibility are specific to their own environment and configuration, and cloud providers have little insight or control over how users operate in those areas. By the same token, users do not

[65] Ariel Levite and Gaurav Kalwani, Cloud Governance Challenges: A Survey of Policy and Regulatory Issues, Carnegie Endowment for International Peace (Nov. 9, 2020), https://carnegieendowment.org/2020/11/09/cloud-governance-challenges-survey-of-policy-and-regulatory-issues-pub-83124.
[66] Id.
[67] Cloud Security Alliance, Shared Responsibility Model Explained (Aug. 26, 2020), https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/
[68] Id.
[69] Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo, Broken trust: Lessons from Sunburst, Atlantic Council (March 29, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/

dictate how cloud providers secure their portion of the cloud.[70] The shared responsibility model can help shed light on how cloud providers and FIs limit their exposure to concentration risk.

Measures taken by cloud providers

The major cloud providers take several measures to mitigate the possibility of any single point of failure in their own infrastructure. Two key elements of their strategy are spreading infrastructure across different "availability zones" and regions.[71]

Availability zones are physically separate locations within a specific region that are isolated from each other using redundant networking, connectivity, and power. By compartmentalizing their own infrastructure and services into redundant, isolated availability zones, major cloud providers reduce the impact that a failure at one location will have on the capacity and availability of their services. If one availability zone is affected, the cloud provider's services, capacity and availability can be supported by remaining availability zones. FIs, or third parties that offer cloud-based services to FIs, can design and operate their cloud-based applications to run synchronously across availability zones without interruption.[72]

In addition to the use of availability zones, which are located in the same region, major cloud providers also locate data centers in different regions, which provides even greater physical isolation from one region to another. This geographic diversity ensures that even major physical catastrophes, like flooding and earthquakes, can be weathered by cloud users without significant disruption. For critical functions that require high levels of availability and resiliency, FIs can take advantage of a cloud provider's distributed regional architecture to ensure that applications or data are consistently available by configuring those functions so that they are spread across the cloud provider's different regions.[73]

Measures taken by financial institutions

FIs also take different approaches to mitigating the risk of disruption and ensure business continuity. As noted above, FIs can distribute processes and data across a cloud provider's different availability zones or regions, allowing them to build applications that can be online even if a particular data center or region experiences a disruption.[74]

---

[70] Cloud Security Alliance, Shared Responsibility Model Explained (Aug. 26, 2020), https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

[71] Although these elements are common to the major cloud providers, their specific implementation varies between different providers. See Amazon, Regions and Availability Zones, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/; Google, Regions and Zones, https://cloud.google.com/compute/docs/regions-zones; Microsoft, What are Azure regions and availability zones?, https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview.

[72] Amazon Web Services, AWS Global Infrastructure (last accessed April 14, 2023) https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=1.

[73] Amazon Web Services, Regions and Availability Zones (last accessed April 14, 2023), https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2.

[74] Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals,* 10.

To protect themselves against lock-in, FIs should consider what impediments may exist which limit their ability to move applications and data off of a cloud provider's infrastructure without unreasonable cost or difficulty. This needs to be considered at both the level of an individual application or workload, as well as the overall relationship with a cloud provider. In general, major cloud providers offer the functionality necessary to move applications and data from one cloud provider to another, or to an on-premises environment at the discretion of the FI. However, factors such as contractual terms, commercial commitments, or the lack of comparable services or features at an alternative provider, may increase the switching cost – expense, time, and effort – of moving between providers. Increasingly, FIs are developing "exit strategies," which outline the different impediments that exist to seamlessly moving applications and data off of a particular cloud service provider, and the steps they will take – both proactive and reactive – to mitigate the impact of those impediments should the FI choose or need to migrate away from the cloud provider. One example of a proactive measure is mandating the use of open-source and open standards to avoid getting locked-in to a particular vendor's proprietary format. The exit strategy also typically defines how the FI will monitor certain key risk indicators (e.g., performance against service level agreements, their commercial relationship with the cloud provider, reputational risks) and what might trigger the FI to initiate the exit plan for moving applications or data off of the cloud provider.

Another strategy that some FIs have employed to mitigate concentration risk is the use of hybrid cloud—migrating applications suited for the cloud while keeping other components in on-premises data centers—so that on-premises infrastructure is used for critical infrastructure or as backup in the event of disruption. Other FIs take a multi-cloud approach, using different cloud providers for different types of workloads, or architecting workloads to be portable between cloud platforms (e.g., through the use of containers). However, the use of a multi-cloud strategy is not without its challenges. To implement a multi-cloud configuration, an FI must build (or rely on another third party to build) a solution for managing applications and data in multiple clouds. This does not eliminate risk; it just transfers it from an individual cloud provider to the FI or a different third-party provider.[75] The use of multiple cloud providers also requires an FI to train staff and implement controls for different cloud environments.[76] A multi-cloud strategy can also potentially introduce additional points of failure that need to be continuously managed and tested to ensure they work when needed (e.g., in the event of an outage). An unintended consequence of a multi-cloud strategy is the standardization on the "lowest common denominator" of capabilities across different clouds, resulting in less-than-optimal cloud usage.

Multi-cloud strategies have also been suggested as a way of increasing FIs' operational resiliency, by enabling them to move processes and data from one cloud provider to another in the event of a disruption. While "multi-cloud failover" may be possible in theory, it is likely to be difficult to implement in practice given the level of complexity as well as

[75] Stratechery, IBM's Old Playbook (Oct. 29, 2018), https://stratechery.com/2018/ibms-old-playbook/
[76] Microsoft, Concentration Risk: Perspectives from Microsoft (Sept. 2020), https://azure.microsoft.com/mediahandler/files/resourcefiles/concentration-risk-perspectives-from-microsoft-/Concentration_Risk_Perspectives_092020.pdf.

factors such as contractual commitments, licensing, and data portability. As a result, leading analysts recommend against such an approach for increasing operational resiliency.[77]

Regarding multi-cloud, the recent US Treasury report refers to the financial sector feedback that multi-cloud (called 'multi-vendor, single use-case deployment in the report), is too technically complex and resulting operational risk was too high.[78] MAS also caution FIs about the added complexity of operating in a multi-cloud environment.[79]

PART III: REGULATORY FRAMEWORKS FOR MANAGING "CONCENTRATION RISK"

This section outlines the regulatory and supervisory frameworks intended to address potential concentration risks in the financial sector. The focus of this section is the U.S. regulatory framework; it then considers approaches taken outside the United States.[80]

a. The U.S. regulatory framework

The regulatory and supervisory requirements governing the use of technology service providers by FIs in the United States differs based on the nature of the institution, its regulator, and the regulator's statutory authority. U.S. banking institutions are regulated and supervised by the federal banking regulators—the Federal Reserve Board of Governors, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (the OCC). Participants in securities and derivatives markets are subject to the regulation and oversight of the Securities & Exchange Commission (the SEC) and the Commodity Futures Trading Commission (the CFTC).

All of these federal regulatory agencies, for example, require at least some FIs within their jurisdiction to notify them of changes to their relationships with third-party service providers. Banks are required by statute to notify the appropriate federal banking agency of the existence of the service relationship within thirty days of the start of the relationship.[81] The federal banking agencies have implemented the notification requirement in different ways: the FDIC has developed a form for FDIC-supervised banks on which to report the

[77] Lydia Leong, Multicloud failover is almost always a terrible idea, Gartner (Oct. 14, 2021), https://blogs.gartner.com/lydia_leong/2021/10/14/multicloud-failover-is-almost-always-a-terrible-idea/; Lydia Leong, Improving cloud resilience through stuff that works, Gartner (Oct. 21, 2021), https://blogs.gartner.com/lydia_leong/2021/10/21/improving-cloud-resilience-through-stuff-that-works/.

[78] *See* U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*, at 6, 26 (2023) https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

[79] Monetary Authority of Singapore, *Advisory on Addressing the Technology and Cyber Security Risks Associated With Public Cloud Adoption* (June 1, 2021), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Cloud-Advisory.pdf.

[80] For a detailed overview of U.S. regulatory framework as it relates to cloud adoption more generally, see the Treasury Department's recent report on cloud adoption in the financial services sector: U.S. Dept. of Treasury, The Financial Services Sector's Adoption of Cloud Services (2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

[81] 12 U.S.C. § 1867(c)(2).

information, while the OCC requires banks to maintain a current inventory of all outsourcing relationships that is available for examination upon OCC's request.[82]

Other financial regulators have implemented notification requirements through regulation. The SEC requires certain securities exchanges, trading platforms and self-regulatory organizations to report quarterly on completed, ongoing and planned material changes to their technological systems, including relationships with third-party services providers.[83] And certain entities registered with the CFTC are required to inform the CFTC of planned changes to their automated systems that impact reliability, security, or capacity and risk analysis and oversight programs.[84]

Direct oversight of technology outsourcing and third-party service providers

The federal banking agencies have statutory authority under the Bank Service Company Act (the BSCA) to subject services provided by technology services providers to regulation and examination to the same extent as if the services were performed by the bank itself.[85] The federal banking agencies coordinate their supervision of banks and their technology service providers through the Federal Financial Institutions Examination Council (FFIEC), whose members include the three federal banking regulators as well as the National Credit Union Administration, Consumer Financial Protection Bureau and representatives from state regulatory agencies. The FFIEC has published guidance on technology outsourcing by banks and supervision of technology service providers.[86] Among other issues, the FFIEC's guidance addresses concentration risks: an FFIEC statement on cloud security, for example, encourages each FI that plans to use cloud services to determine their "comfort with its dependence on … the cloud service provider."[87]

The federal banking agencies have also issued their own guidance for FIs' management of risk, including concentration risk, associated with outsourcing to technology service providers. The Federal Reserve's guidance on outsourcing risk, for example, directs FIs to consider the concentration risks that arise "when outsourced services or products are

[82] FDIC, *Financial Institution Letter Re: Bank Technology Bulletin*, FIL-50-2001 (June 4, 2001), https://www.fdic.gov/news/news/financial/2001/fil0150.html; OCC, *Risk Management Guidance*, OCC Bulletin, 2013-29, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[83] 17 CFR § 242.1003.

[84] 17 CFR § 37.1401(f), 38.1051(f), 39.18(h)(1)–(2), 49.24(h).

[85] 12 U.S.C. § 1863.12 U.S.C. § 1867(c)(1); 12 U.S.C. § 1464(d)(7)(D). Other federal financial regulatory agencies do not have the same direct examination and regulatory authority over third-party service providers.

[86] The FFIEC publishes principles-based guidance on IT risk management for regulators and financial institutions in the form of IT Booklets. These booklets include guidance on banking institutions' responsibilities with respect to IT outsourcing, as well as guidance for regulators' supervision of technology service providers. FFIEC, *Outsourcing Technology Services*, FFIEC: IT Examination Handbook (June 2004), https://ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf; FFIEC, *Supervision of Technology Service Providers*, FFIEC: IT Examination Handbook (Oct. 2012), https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

[87] Federal Financial Institutions Examination Council, Joint Statement on Security in a Cloud Computing Environment, https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf.

provided by a limited number of service providers or are concentrated in limited geographic locations."[88]

The federal banking agencies have also issued proposed guidance to FIs on managing risk associated with third-party relationships. This guidance calls on FIs to monitor and control micro- level concentration risks, including by conducting independent reviews that assess the adequacy of their processes for monitoring concentration risks "that may arise from relying on a single third party for multiple activities or from geographic concentrations of business."[89]

In addition to its policy-setting role, the FFIEC coordinates the supervisory program for the largest, systemically important technology service providers: significant service providers (SSPs), formerly multi-regional data processing services (MDPS) firms.[90] Since 2014, the federal banking agencies have increased their scrutiny of these third-party service providers. A technology service provider is considered for the SSP/MDPS program when it processes "mission-critical"[91] applications for a large number of financial institutions (1) that are regulated by more than one agency, thereby posing a high degree of systemic risk or (2) from a number of data centers located in different geographic regions. Service companies in the /SSP/MDSP program are deemed to pose a significant risk to the banking system if one or more has operational or financial problems or fails.[92]

According to a report from the Inspector General of the Federal Reserve Board of Governors, there were fifteen firms with the MDPS designation as of 2017.[93] The report documented numerous deficiencies in the banking agencies' administration of the MDPS program, including a lack of knowledge about the universe of potential MDPS firms due to the agencies' lack of enforcement of the BSCA's notification requirement. According to the report, this failure to enforce has limited supervisory agencies' knowledge as to which service providers banks use for various applications, mission-critical or otherwise.[94]

[88] Board of Governors of the Federal Reserve System: Divisions of Banking Supervision and Regulation and Consumer and Community Affairs, Guidance on Managing Outsourcing Risk (Dec. 5, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.

[89] Federal Reserve System, the Federal Deposit Insurance Corporation, and the Comptroller of the Currency, Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182 (July 19, 2021), https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management#citation-20-p38194

[90] FFIEC, *Supervision of Technology Service Providers*, 4.

[91] According to the FFIEC, "[a]n application or system is mission-critical if it is vital to the successful continuance of a core business activity. An application also may be mission- critical if it interfaces with a designated mission-critical system. Products of software vendors also may be mission-critical." Id. at 12.

[92] Id.

[93] Office of the Inspector General, Federal Reserve Board, *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing*, 8 (April 2017), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-apr2017.pdf.

[94] Id, 7-10.

Potential designation of cloud providers as "systemically important" or "critical" providers

Certain policymakers and academics have suggested that cloud providers with a large number of financial institution clients could be subjected to enhanced supervision as financial market utilities or a form of critical third-party service provider.[95]

For example, the Dodd-Frank Act authorizes the Financial Stability Oversight Council (FSOC) to designate any person that manages or operates a multilateral system for transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions as a "systemically important financial market utility" (SIFMU)[96] if its failure or disruption could threaten the stability of the U.S. financial system by creating or increasing liquidity or credit risk.[97] SIFMUs are subject to enhanced legal requirements and subjected to more exacting levels of supervision. Under this mandate, FSOC has designated eight companies operating as clearinghouses, exchange platforms, and custodians as SIFMUs.[98] Advocates of designating major cloud providers as SIFMUs argue that they have "become an essential element of [the] modern banking system."[99]

Alternately, certain major cloud providers could be designated "critical third-party providers" subject to enhanced supervision by one or more financial market regulators to the extent they provide "critical" cloud services to FIs at sufficient scale that their failure or disruption could threaten the stability of the financial system. Such a regime would resemble the European Union's Digital Operational Resilience Act discussed in the next section. The potential designation of major cloud providers as SIFMUs or critical third-party providers is analyzed in Part IV.

b. Regulatory frameworks in international jurisdictions

While the U.S. regulatory framework for managing and monitoring IT outsourcing risk in the financial sector largely predates the shift to cloud services, other jurisdictions have proposed or adopted updated frameworks that expressly contemplate the use of cloud services by financial institutions, including the concentration risks that such use might pose.

Financial institutions' responsibility for managing concentration risk

Several jurisdictions have, like the United States, adopted regulatory frameworks that place the onus of assessing and managing the risk—including concentration risk—associated with an FI's outsourcing on the FI. For example, outsourcing guidance published

[95] *See* U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*, at 41, 44, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.
[96] Pete Schroeder, *U.S. House lawmakers ask regulators to scrutinize bank cloud providers*, Reuters (Aug. 23, 2019), https://www.reuters.com/article/us-usa-congress-cloud/u-s-house-lawmakers-ask-regulators-to-scrutinize-bank-cloud-providers-idUSKCN1VD0Y4.
[97] 12 U.S.C. § 5462(6)(A), (9).
[98] Federal Reserve Board, *Designated Financial Market Utilities* (Jan. 2015), https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.
[99] Schroeder, *U.S. House lawmakers ask regulators to scrutinize bank cloud providers* (cited in note 95).

by the U.K.'s Prudential Regulation Authority directs regulated FIs to periodically assess and take reasonable steps to manage concentration and lock-in risks. This can be from multiple arrangements with the same service provider, supply chain dependencies that cause FIs to rely indirectly (through multiple service providers) on the same subcontractor, and concentration of dependencies in a single geographical location or jurisdiction.[100]

Similarly, outsourcing guidance issued by the European Banking Authority (EBA) direct FIs to consider, as part of the pre-outsourcing risk assessment, concentration risks arising from outsourcing to a dominant service provider that is not easily substitutable or from multiple outsourcing arrangements with the same service provider.[101] The European Securities and Markets Authority's (ESMA) cloud-specific guidelines go even further: they direct regulated FIs to consider not just concentration risks within an individual FI, caused by multiple outsourcing arrangements with the same service provider, but also possible concentration within the broader European financial sector as a result of multiple FIs using the same service provider or a small group of service providers.[102]

Outsourcing guidelines published by the Monetary Authority of Singapore (MAS) affirms that financial institutions that use cloud-based services are "ultimately responsible and accountable for maintaining oversight" and "managing the attendant risks" of adopting cloud services.[103] This principle is echoed in detailed guidance on cloud adoption subsequently published by the MAS,[104] which explicitly addresses "lock-in" and "concentration risk". The cloud adoption guidance directs FIs to consider mitigating lock-in risks by adopting cloud portability or interoperability solutions and relying on open standards for data and software interfaces to facilitate redeployment of cloud workloads to on-premises or alternative cloud infrastructures. In the case of concentration risk mitigation, the cloud adoption guidance notes that FIs may consider implementing vendor diversity measures such as a "multi-cloud strategy": the use of services from different cloud providers. However, it also cautions FIs about the added complexity of operating in a multi-cloud environment, such as having adequate resources and appropriate expertise in securing and managing the use of different public cloud services, especially in light of significant differences between cloud service providers..[105]

---

[100] Bank of England, Prudential Regulation Authority, *Outsourcing and third party risk management*, Supervisory Statement SS2/21, Section 5.24 (March 2021). https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

[101] EBA, Guidelines on outsourcing, Section 12.2 par. 66 (Feb. 25, 2019), https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.

[102] ESMA, Guidelines on outsourcing to cloud service providers, par. 21(a)(vii) (Oct. 5, 2021), https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf.

[103] Monetary Authority of Singapore, *Guidelines on Outsourcing*, Section 6.8 (Oct. 2018)

[104] Monetary Authority of Singapore, *Advisory on Addressing the Technology and Cyber Security Risks Associated With Public Cloud Adoption*, par. 38 (June 1, 2021), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Cloud-Advisory.pdf. The cloud adoption guidelines do not specifically define "lock-in" or "concentration risk". In more recent guidance addressing business continuity, MAS describes concentration risk as arising "when there is concentration of people, technology or other required resources" in the same region or when several of an FI's "critical business services and/or functions are outsourced to a single service provider." That guidance outlines additional measures, which are not specific to cloud adoption, that FIs should consider in order to mitigate concentration risk. BCM-Guidelines-June-2022.pdf (mas.gov.sg).

[105] Id, par. 36.

Direct oversight of cloud providers – DORA

Until recently, most financial regulators lacked the authority to directly supervisory technology service providers—including to monitor potential concentration risk.[106] To address that lack of authority, several jurisdictions have proposed or adopted frameworks that would establish mechanisms for direct oversight of critical technology providers including certain cloud providers by financial regulators. In December 2022, the European Union formally adopted the Digital Operational Resilience Act (DORA). [107] DORA is a comprehensive framework for digital operational resilience for financial entities in the E.U., with a significant portion devoted to managing third-party risk associated with the outsourcing of information and communication technologies (ICT).[108]

The third-party risk provisions have two components: a set of key principles governing financial entities' management of third-party ICT risk and a framework for financial supervisory agencies' oversight of third-party ICT service providers designated as "critical". Critical third-party service providers (CTPPs) are designated as such based on the several criteria, including the potential systemic impact on the provision of financial services if the service provider were to experience a large-scale operational failure and the importance of the financial institutions that rely on the service provider.[109] Although DORA's CTPP provisions are not specifically limited to cloud service providers, they were intended to address potential risks—including concentration risks—arising from cloud adoption in the financial sector.[110]

DORA establishes an E.U.-level oversight mechanism pursuant to which each CTPP would be subject to direct, ongoing oversight from one of the E.U. Supervisory Authorities (its "Lead Overseer").[111] This Lead Overseer is responsible for assessing the CTPP's risk management framework with respect to its financial sector customers. To carry out these responsibilities, the Lead Overseer is vested with broad authority to request information and documents and to conduct investigations and inspections of the CTPP.[112] DORA also empowers the Lead Overseer to issue specific, substantive recommendations to CTPPs.[113] Of particular note, DORA gives the Lead Overseer the authority to make recommendations regarding the conditions and terms under which a CTPP provides services

---

[106] See Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices*, 33–34 (BIS Dec. 2018); Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, *Regulating and supervising the clouds: emerging prudential approaches for insurance companies*, FSI Insights on policy implementation No. 13, 26–28 (BIS Dec. 2018), https://www.bis.org/fsi/publ/insights13.pdf.

[107] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014* (Sept. 29, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.

[108] See generally Program on International Financial Systems, *The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies* (Aug. 2021), https://www.pifsinternational.org/the-e-u-s-digital-operational-resilience-act-cloud-services-financial-companies/.

[109] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014* at Article 28(2) (Sept. 29, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN. .

[110] Id, Preamble, pars. 28-29.

[111] Id, Articles 29-30.

[112] Id, Articles 31(1)(a)-(b), 32-34.

[113] Id, Articles 31(1)(d), 35.

to FIs which the Lead Overseer deems relevant for preventing potential single points of failure and for minimizing the possible systemic impact of concentration risk arising from the use of technology service providers.[114]

In addition to these powers, the Lead Overseer is authorized to impose a penalty on the CTPP—equal to one percent of the CTPP's average daily worldwide turnover—if it does not comply with the Lead Overseer's requests for information, exercise of its investigation and inspection powers, or requests for follow-up reports on its substantive recommendations.[115] Finally, DORA would restrict the use of non-E.U. third-party service providers that would be designated as critical if established in the E.U.[116]

Direct oversight of cloud providers – other proposals

Other jurisdictions have also considered or are considering proposals that would give financial regulators direct regulatory and supervisory oversight over technology service providers, including cloud providers. In South Korea, a reform plan published by the Financial Services Commission has served as the basis of proposed legislation that would subject "major outsourcing companies"—third-party service providers, including cloud providers, whose services have a material impact on the stability and reliability of electronic financial transactions—to direct supervision by Korean financial regulators.[117] Under the proposed legislation, financial regulators would be able to request information from and conduct investigations of those "major" third-party service providers. Financial regulators would also be empowered to issue corrective orders based on their supervisory activities and to take additional enforcement measures against service providers if they fail to comply with those orders.[118]

The United Kingdom is actively considering legislation that would give the Treasury direct regulatory oversight of "critical" third-party service providers, such as cloud providers, the failure or disruption of which could threaten the stability of the U.K.'s financial system.[119] The impetus for the legislation was, in part, the view that financial regulators' current powers are insufficient to tackle the systemic risk originating from "a concentration in the provision of critical services by on third party to multiple firms."[120]

The legislation would authorize the Treasury to designate, in consultation with financial regulators and "other persons as the Treasury considers appropriate", certain third-party service providers as "critical", giving financial regulators a range of powers with respect

[114] Id, Articles 31(1)(d)(ii).
[115] Id, Article 31(4)-(8).
[116] Id, Article 28(9).
[117] *Proposed amendments to the Electronic Financial Transactions Act* (Nov. 27, 2020), http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2Y0P1Y1P2W7K1W7I5D8X0O7Q2R3T3; Kim & Chang, *New Regulations Concerning Cloud Computing: Expected Impact on Cloud Computing Service Providers* (Dec. 4, 2020), https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=22427.
[118] Id.
[119] U.K. Parliament, Financial Services and Markets Bill (Dec. 8, 2022), https://bills.parliament.uk/publications/49063/documents/2625; HM Treasury, *Critical third parties to the finance sector: policy statement* (June 8, 2022), https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement#the-critical-third-party-regime.
[120] Id, par. 1.10.

to services those critical third parties provide to the financial sector.[121] Those powers would include the regulatory authority to make rules setting minimum resilience standards for critical third parties with respect to any services they provide to the U.K. financial sector and the supervisory power to assess whether those minimum resilience standards are met.[122] Financial regulators would also be granted the power to direct critical third parties to take (or refrain from taking) specific actions, and enforcement powers ranging from the ability to publicize failings to the authority to restrict the provision of services by critical third parties to financial institutions.[123]

PART IV: POLICY RECOMMENDATIONS

This section outlines several recommendations for policymakers intended to mitigate potential concentration risks associated with FIs' transition to the cloud.

a. Focus on information gathering and sharing to monitor concentration risks

To monitor concentration risk, supervisory authorities must be able to determine which regulated FIs rely on which cloud providers and for which functions. Supervisory authorities should therefore enforce existing notification requirements that mandate reporting by FIs of outsourcing arrangements, including the use of cloud-based services. Supervisory authorities should also consider how FIs' notification requirements can be tailored to make the reports more useful—for example, authorities can develop a standardized reporting format, or even a central registry, to enhance consistency and comparability of FIs' reported information.[124] These reports would enable supervisory authorities to develop a view of dependencies in the financial system, assess potential concentration risks, and respond effectively to disruptions.

Concentration risk can also be addressed through specific information gathering, information sharing and coordination among FIs, cloud providers, and supervisory authorities. Requirements that FIs and cloud providers share information on risk assessments, contingency plans and best practices for security and resiliency can help mitigate systemic risk by reducing uncertainty and improving collective learning by FIs and their supervisors. However, these efforts should recognize that the cloud service providers do not have visibility of their FI customer workloads.

Likewise, supervisory authorities should leverage existing forums for coordination on cyber risk and financial system resilience. In the United States, for example, the financial regulators, including the federal banking agencies, the SEC and the CFTC, have established information sharing protocols. In addition, FIs and federal and state regulators have

[121] Id, par. 1.13.
[122] Id., par. 1.16-1.18.
[123] Id, par. 1.19.
[124] HM Treasury, *Critical third parties to the finance sector: policy statement* (June 8, 2022), https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement#the-critical-third-party-regime. They should also take account of the risk that such information would be a potential target for bad actors.

established information sharing platforms to address issues of cybersecurity in the financial sectors.[125] And the U.S. Treasury Department has sponsored a series of exercises, developed in collaboration with FIs and other government agencies, to prepare financial sector participants and regulators for various cyber incidents.[126]

At the international level, the International Organization of Securities Commissions (IOSCO), the international coordinating body for securities regulators, and the Committee on Payments and Market Infrastructures (CPMI), which sets international standards for payments, clearing and settlements, have worked together to release cyber risk guidelines for financial market utilities.[127] In addition to these standard-setting bodies, financial regulators can collaborate through the Financial Stability Board.[128]

b. Clarify and tailor concentration risk guidance

Cloud adoption is clearly at a nascent stage in the financial sector with only three percent of core systems, such as bank-end process and systems that manage customer interactions throughout the bank having been migrated to the cloud. Therefore, even if the provision of cloud service providers to FIs were concentrated, the potential impact of cloud service providers on the financial system as a whole may be limited, since only a very small share of core systems rely on cloud services.

As cloud adoption by FIs increases, and FIs and their regulators continue to develop their understanding of the risks associated with the use of cloud services, supervisory authorities should clarify their guidance with respect to potential concentration risks. Regulators should recognize that, from a financial stability perspective, concentration risk is not invariably problematic. The potential risks of concentration must be weighed against the benefits of enhanced security and resilience, scale and quality achieved by major cloud providers.

Moreover, regulatory requirements and supervisory guidance should be tailored to specific risks, and must not adopt a one-size-fits-all approach. For example, the complexity and operational risk associated with a multi-cloud approach may render it an inappropriate solution for most FIs.

---

[125] FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC), http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html; FBIIC, Mission and History, https://www.fbiic.gov/mission-history.html.

[126] Shaun Waterman, Bank Regulators Briefed on Treasury-Led Cyber Drill, FedScoop, July 20, 2016, https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016/; Financial Services Information Sharing and Analysis Center, Exercises Overview, https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf.

[127] CPMI-IOSCO. (2016). Guidance on Cyber Resilience for Financial Market Infrastructures, https://www.bis.org/cpmi/publ/d146.pdf.

[128] Financial Stability Board, Third-party dependencies in cloud services: Considerations on financial stability implications (Dec. 9, 2019), https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

Clarify respective responsibilities of financial institutions and cloud providers

Part of clarifying guidance involves delineating the division of responsibilities between regulated FIs and cloud providers. As described above, major cloud providers adhere to a "shared responsibility" model for security and resilience.[129] The shared responsibility model has several implications for concentration risk. Unlike a traditional on-premises vendor, a cloud provider will not have visibility into what sorts of workloads are being deployed on its infrastructure and its usage that limits the information that cloud providers can directly provide to supervisory authorities.

c. The importance of cross-border coordination and solutions

A lack of consistent policies and regulations across jurisdictions makes it difficult for FIs and cloud providers to comply with concentration risk-related requirements and mitigation guidelines, and for supervisors in different jurisdictions to coordinate in the event of a disruption. In addition, direct oversight of cloud providers in each jurisdiction may be redundant. It is therefore important that regulators arrive at shared principles for monitoring and mitigating concentration risk resulting from cloud adoption in the financial sector, and work to coordinate responses to disruptions that affect FIs in different jurisdictions.[130]

There are several existing forums and international bodies that can be leveraged to facilitate cross-border coordination and solutions, including the regular E.U.–U.S. Joint Financial Regulatory Forum, which brings together European and U.S. financial regulators,[131] as well as the FSB, IOSCO and CPMI.[132]

Financial regulators should also recognize the important role of cloud providers' global and regional diversity in ensuring the resiliency of cloud services—mitigating the potential for a single point of failure. Cloud providers' multi-jurisdictional infrastructure forms a critical part of the resiliency and availability advantage offered by cloud services. Financial regulators should weigh that benefit when considering rules governing data residency.

Data localization requirements that interfere with the ability of FIs to make use of that out-of-jurisdiction infrastructure can potentially affect resiliency—especially in smaller jurisdictions, where there is less (if any) in-jurisdiction infrastructure. Such requirements result in decisions about where to store data and run applications being driven by the regulatory requirements of individual cloud customers, instead of security or resiliency considerations. Data localization requirements can arguably increase concentration risk by limiting competition from cloud providers that do not have in-jurisdiction infrastructure, increasing reliance on a smaller set of cloud providers.

---

[129] See Section II.D.
[130] See Section IV.A.
[131] The February 2023 forum discussed the U.S. Treasury's recent report on cloud services, DORA, as well as multilateral work on cloud services at the FSB.
[132] See Section IV.A.

d. Ensure that regulatory tools and practices are fit for purpose

Most importantly, financial regulators should ensure that the regulatory tools and practices they utilize to monitor and mitigate potential concentration risks resulting from cloud adoption are fit for purpose. In the United States, for example, the possibility that cloud providers may become critical to the operations of the financial market has led to calls to designate certain major cloud providers as SIFMUs, or to designate them as "critical third-party providers" and hold them to similar standards.[133]

However, the statutory criteria for SIFMU designation, as well as the regulatory requirements applicable to SIFMUs, all focus on *financial* risk, such as liquidity and credit risk, posed by a SIFMU's operations or failure.[134] In contrast, the potential risks that cloud providers may pose to the financial sector are not financial in nature. Cloud service providers serve a technical, not financial, role in the financial services sector. Regulators should not use tools developed to address systemic financial risks to address the risks that a potential operational disruption at a cloud service provider may pose to the financial system.

Given financial regulators' current mandate, resourcing levels and expertise, it is important that their priority remain FIs' usage of cloud services, not the broader usage of cloud services outside of the financial sector. Working with FIs and cloud service providers—and with one another— financial regulators can assess how cloud services are changing how FIs use technology and understand the benefits and risks of cloud adoption.

[133] See Section III.A.
[134] 12 U.S.C. § 5463(a)(2)).

Program on International Financial Systems (PIFS)
134 Mount Auburn Street, Cambridge, MA 02138
www.pifsinternational.org