PIF S

Program on International Financial Systems

Cloud Computing in the Financial Sector: A Global Perspective

Hal S. Scott, Emeritus Nomura Professor of International Financial Systems, Harvard Law School

John Gulliver, Executive Director, Program on International Financial Systems

Hillel Nadler, Senior Research Fellow, Program on International Financial Systems

JULY 2019

The Program on International Financial Systems (PIFS) is a 501(c)(3) organization that hosts international symposia, executive education programs and special events that foster dialogue and promote education on issues impacting the global financial system. PIFS also conducts research 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. Today, PIFS hosts three annual international symposia, US-Japan (21 years), US-Europe (17 years), and US-China (16 years).

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

Cloud Computing in the Financial Sector: A Global Perspective*

Hal S. Scott, Emeritus Nomura Professor of International Financial Systems, Harvard Law School

John Gulliver, Executive Director, Program on International Financial Systems

Hillel Nadler, Senior Research Fellow, Program on International Financial Systems

* The authors wish to thank the staff of PIFS, and in particular Eugenio Briales and Harrison Fregeau, for their contributions to this report.

As financial institutions move their operations, including core functions, to the cloud, financial regulators have begun to issue regulations and informal guidance addressing the use of cloud services in the financial sector. These are typically based on the regulator's existing framework for outsourcing by a financial institution to third-party technology providers, under which the risks associated with outsourcing and the supervision of third-party providers are primarily the responsibility of the financial institution. This report provides background on the use of cloud computing in the financial sector, reviews existing regulatory and supervisory frameworks for cloud use by financial institutions, and recommends improvements to those frameworks that could reduce obstacles to more widespread cloud adoption by financial institutions.

Contents

1 Introduction

Cloud computing refers to the use of computing resources over a network (such as the internet) in a manner that scales automatically with demand and allows customers to pay based on their usage. Unlike traditional "on-premises" computing, which typically features the use of proprietary data centers owned or controlled by the organization that they serve, cloud computing involves the provision of relatively standardized services by one service provider to many different customers on a large scale. The cloud model enables customers to outsource the administration of technology infrastructure to cloud service providers and to access computing resources without the up-front capital expenditures necessary for traditional data centers.

Financial institutions, ranging from banks, asset managers and insurers to payments systems providers and securities depositories, currently use cloud services for everything from non-critical services such as email management and app development to core functions such as payment processing and data storage. This report seeks to inform, in three primary ways, the effective regulation and supervision of cloud use by financial institutions:

1. **Providing background on the use of cloud computing by financial institutions and the associated benefits and risks.** We find that the potential benefits of cloud computing are significant: a move to the cloud can enable financial institutions to innovate and deliver new products and services to market more quickly, while also increasing their security and operational resiliency. In addition, the use of cloud computing can facilitate data analytics at massive scale, improving risk management and opening new regulatory frontiers. Though cloud computing may also present some genuine (and in some cases, novel) risks to financial institutions, cloud service providers and financial institutions have taken an active role in addressing those risks.

2. **Reviewing the existing regulatory and supervisory frameworks for the use of cloud computing by financial institutions.** Our comprehensive review of the regulatory and supervisory frameworks currently in place focuses on the United States and the European Union. It is organized around common themes addressed in regulation and supervisory guidance, and highlights points of difference between various jurisdictions. The review should be informative both for international standard setting organizations as well as regulatory agencies that are developing new frameworks for technology outsourcing by financial institutions or are revisiting their existing frameworks.[1]

[1] As these regulatory and supervisory requirements are highly technical, a detailed evaluation is beyond the scope of this summary report; we do not draw specific conclusions as to the necessity or sufficiency of particular requirements.

3. **Recommending three courses of action in order to reduce obstacles to more widespread cloud adoption by financial institutions.** Our recommendations focus on reducing regulatory barriers to cloud adoption by streamlining the due diligence and monitoring process, improving coordination between regulators in different jurisdictions, and continuing to monitor and assess potential industry-level risks of cloud use by financial institutions. We recommend that financial regulators: (i) recognize the utility of having financial institutions jointly audit their shared cloud service providers; (ii) work together to resolve cross-border issues presented by cloud computing on the basis of shared principles; and (iii) continue to engage in a risk-based dialogue on potential industry-level risks posed by widespread cloud adoption by financial institutions.

2 Financial institutions and cloud computing

a. Background

From data centers to the cloud

Until the middle of the twentieth century, banking technology was mostly manual. Banks started using computers in the 1950s, with the introduction of the first large commercial computers. In the 1960s, computer technology began to catch on rapidly throughout the financial industry: between 1963 and 1968, the proportion of commercial banks using on-premises or off-premises computers rose from less than one-in-ten to almost half.[2] Initially, computers were used for check processing; later they were used for electronic funds transfer, which enabled the establishment of automated clearinghouses for interbank settlements and ATMs to process financial transactions.[3]

Since banks first began to use computers, they have relied on information technology infrastructure—whether in-house mainframes or external data centers—owned or controlled by non-bank technology companies (in some cases, data centers were maintained in shared facilities by service companies that were co-owned by banks).[4] In the 1980s and 1990s, banks started to use personal computers to interact with that technology infrastructure, replacing older terminal technology; by the mid-1990s, a greater proportion of workers in finance used computers than in any other industry.[5] The use of personal computers enabled access to external networks using internet and email. And the internet had another effect: increasing the number and quality of remote services that banks could offer customers, which in turn placed additional burdens on their IT infrastructure.

To cope with increasing IT demands and in order to offer better and more innovative remote and mobile services to clients, financial institutions have begun to turn from proprietary IT infrastructure to the cloud, using cloud services to support a variety of functions ranging

---

[2] See Horst Brand and John Duke, *Productivity in commercial banking: computers spur the advance*, 105 Monthly Lab. Rev. 19, 22-23 (December 1982).

[3] See id at 23-24.

[4] See Douglas Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals*, Microsoft 8 (2017), available at https://download.microsoft.com/download/0/D/6/0D68AE95-6414-4074-B4B8-34039831E2BF/Introduction-to-Cloud-Computing-for-Legal-and-Compliance-Professionals.pdf; 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.

[5] See Teresa L. Morisi, *Commercial banking transformed by computer technology*, 119 Monthly Lab. Rev. 30, 31 (August 1996).

from mobile banking applications to processing credit card transactions and other payments, loan applications, and insurance claims.[6] According to analysis from the U.S. Treasury Department and industry research, migration of core financial services activities to the cloud is expected to increase materially over the next decade, driven by the need to process massive amounts of data and to offer mobile-first digital banking services.[7]

Cloud service models

As noted earlier, cloud computing involves the use of computing resources over a network—usually the internet, but in some cases a private network—in a manner that is scalable with demand.[8] This general description, however, can obscure the fact that cloud computing encompasses a variety of service models. The nature and degree of control and risk that a financial institution assumes when it uses cloud services varies depends on the service model that is adopts.

Cloud services can be divided into three basic models: infrastructure, platform, and software. Infrastructure-as-a-service (IaaS) involves the use of computational infrastructure, such as servers, storage capacity or networking. In the IaaS model, cloud providers control the underlying cloud infrastructure while the customer controls everything from the operating systems to the applications that run on that infrastructure. At the other end of the spectrum, the software-as-a-service (SaaS) model allows customers to run software developed by a third-party service provider on remote cloud servers. The platform-as-a-service (PaaS) model offers more structure than the IaaS model but more flexibility than the SaaS model; it enables the development and use of software by the customer on app hosting and development infrastructure offered by a cloud service provider.[9] Different types of cloud services can be layered on top of each other. For example, fintech startups that offer SaaS services

---

[6] For more detail on the differences between traditional outsourcing and cloud computing, see generally W. Kuan Hon and Christopher Millard, *Cloud Computing vs. Traditional Outsourcing – Key Differences*, 23 Computers & Law 4 (Oct./Nov. 2012), available at https://ssrn.com/abstract=2200592.

[7] See Steven T. Mnuchin and Craig S. Phillips, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation – Report to President Donald J. Trump, Executive Order 13772 on Core Principles for Regulating the United States Financial System* (U.S. Treasury Report), U.S. Department of the Treasury, 48-49 (2018), available at https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf; PwC, *Financial Services Technology 2020 and Beyond: Embracing disruption*, 22 (2016), available at https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf.

[8] See 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.

[9] See 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.

often build their services on a major cloud provider's IaaS or PaaS service, using basic computing, networking and storage services offered by the cloud provider to provide software services to their clients.[10]

A financial institution's choice of service model will be shaped by both its needs and technical capabilities. Financial institutions with more in-house technical expertise, whether large banks or small fintech startups, may use infrastructure resources to build entirely new applications. Those with less technical expertise are more likely to use the cloud to run software developed by third parties, which is easier to deploy. In fact, some financial institutions that already run sophisticated risk- and asset-management software on cloud infrastructure have begun to offer that software directly to their own clients as a layered cloud service.

Private and public cloud

In addition to offering different service models, cloud providers also offer different deployment models. "Private cloud" refers to cloud resources that are dedicated to a single customer. A private cloud can be hosted on-premises, where it can be managed by the customer directly, or off-premises at the data center of a cloud provider that creates and manages the cloud exclusively for the customer. "Public cloud", unlike private cloud, involves the use of standardized, commoditized cloud infrastructure by multiple different customers.[11]

This report focuses primarily on the use of public cloud: the use of computing resources on infrastructure that is owned and managed by a third party and shared with other customers. The reason for this focus is twofold: (1) public cloud offers unique benefits of standardization and commoditization and the associated economies of scale; and (2) the relationship between financial institutions and public cloud providers is fundamentally different from a traditional outsourcing relationship—financial institutions that use the public cloud share computing resources with thousands, if not millions, of other customers located across many different jurisdictions.

---

[10] See 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).

[11] See Simmon, *Evaluation of Cloud Computing Services Based on NIST SP 800-145* at 12-17 (cited in note 9). "Hybrid cloud" involves the mixed use of private and public cloud—for example, the use of private cloud for storage and processing of sensitive information but public cloud for other information. Cloud service 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 (2019), available at https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf.

b. Benefits of cloud computing

The transition from traditional data centers to the cloud is driven by the significant benefits offered by cloud services. These benefits stem from the availability, on the cloud, of computing resources with improved functionality and reliability and without significant up-front capital expenditures.

Lower costs, increased efficiency

As banking operations have increased in complexity, proprietary data centers have become more expensive. In order to ensure their smooth operation, financial institutions must continually invest in refreshing hardware infrastructure, including infrastructure that exceeds their everyday computing needs. This excess capacity, and the human and organizational resources necessary to manage and maintain it, is necessary to support their highest projected volume requirements—even if that capacity is rarely used.[12]

Cloud technology, by contrast, allows financial institutions to benefit from economies of scale inherent in sharing a cloud provider's vast resources across its many customers. In addition, cloud providers offer their customers the ability to automatically scale up when additional resources are needed and scale down when demand subsides. By offering a utility-like model that makes computing resources available on demand—where customers pay only for resources that they actually use—cloud computing can eliminate the need for costly over-provisioning.[13]

Automation and metering of cloud resources also contribute to lower technology infrastructure costs by transforming large, up-front capital expenditures into smaller, ongoing operational costs.[14] This translates not just to lower costs for purchasing, support and maintenance of technology infrastructure, but also to increasing agility when financial institutions develop new products and services; the cloud's scalability allows financial institutions to test new scenarios, software tools and alternative configurations without a lengthy purchasing and provisioning process.[15] Anecdotal evidence suggests that 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.[16] Lower technology infrastructure

---

[12] See Depository Trust & Clearing Corporation (DTCC), *Moving Financial Market Infrastructure to the Cloud*, 5-6 (May 2017).

[13] See id at 6; Blazheski, *Cloud banking or banking in the clouds?* at 5 (cited in note 4).

[14] See DTCC, *Moving Financial Market Infrastructure to the Cloud* at 6 (cited in note 12); Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals* at 9 (cited in note 4).

[15] See Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services* at 7 (cited in note 10).

[16] See Barb Darrow, *Why Fortune 500 Companies Are Trusting the Cloud More Than Ever*, Fortune (Sep. 13, 2017), available at http://fortune.com/2017/09/13/amazon-microsoft-google-sap-cloud/.

costs can mean lower costs overall,[17] as well as better products and services for end-customers.

Additionally, cloud computing creates a more level playing field between financial institutions of different sizes, by giving small- and medium-sized institutions access to computing resources that were previously only available to larger institutions with the ability to devote significant resources to technology infrastructure.[18] The lower up-front cost of cloud computing also makes it easier for fintech startups to compete with well-established financial institutions, with the potential both for improving services and expanding financial access—particularly to consumers in developing or underserved markets.[19]

Increased security and resiliency

Cloud computing can also be more secure and resilient than traditional platforms. Financial institutions have historically used a mix of technology infrastructures, each typically designed to support a particular set of applications at a given point in time.[20] As banks provided increased internet and mobile access to clients, as well as more flexibility for their internal workforce, those legacy infrastructures became more exposed to cyber threats. That exposure can be severe because many financial institutions are unable to detect penetration of unprotected systems—and even when they are detected, financial institutions are unable to adequately address them due to reliance on manual procedures.[21]

Given the scale at which global cloud providers operate—from hundreds of data centers to transit centers to dispersed development teams—they employ automated mechanisms to detect and remediate issues quickly. Cloud providers can substantially restrict human access

---

[17] See, for example, Jeremy Kahn and Charlie Devereux, *Banks Waking Up to Fintech Threat Throw Billions Into Digital*, Bloomberg News (May 9, 2019), available at https://www.bloomberg.com/news/articles/2019-05-10/banks-waking-up-to-fintech-threat-throw-billions-into-digital ("Shifting to the cloud and changing internal management processes to those most often used by software companies will help the bank realize 30% cost efficiencies.").

[18] Cloud service providers, for example, can enable compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) by offering a secure environment for storing, processing, and transmitting credit card information. See generally, Cloud Special Interest Group, *PCI SSC Cloud Computing Guidelines*, PCI Security Standards Council (April 2018), available at https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

[19] The IMF and World Bank have acknowledged the role of cloud technology in enabling financial access, noting that "third-party providers that offer ancillary services, such as cloud computing and analytics, that underpin many fintech services are reducing the need for large investments by start-ups and are lowering barriers to entry." See World Bank Group and International Monetary Fund, *Bali Fintech Agenda – Chapeau Paper* 17 (Sep. 19, 2018), available at 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.

[20] See Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services* at 12 (cited in note 10).

[21] See DTCC, *Moving Financial Market Infrastructure to the Cloud* at 6 (cited in note 12).

to data, thereby mitigating the risks, such as human error, associated with manual processes.[22]

Although some financial institutions, especially larger ones, devote extensive investment and personnel resources to security, small and medium-sized financial institutions cannot. Major cloud providers, by contrast, are at the forefront of security implementation and research.[23] Cloud platforms are built to support the most stringent security requirements: customers can establish and enforce security models in the cloud using best practices, standards, data encryption and activity logging.[24]

Due to the distributed nature of storage and processing in the cloud, as well as the greater computing resources available to cloud providers compared to individual financial institutions, the cloud can also provide financial institutions with greater operational resiliency.[25] For example, cloud providers can handle attempts to disrupt a financial institution's operations (such as a distributed denial-of-service, or "DDoS", attack) in ways that would be difficult for individual financial institutions to deal with on their own. A DDoS attack attempts to overwhelm a financial institution's computing resources with increased message traffic; cloud providers make it possible for the financial institution to automatically scale up capacity and redirect incoming traffic to maintain availability.[26]

Similarly, by enabling financial institutions to distribute processes and data across different data centers, cloud platforms allow them to build applications that must be online constantly, even if a particular data center—or an entire region—experiences a disruption.[27] Cloud providers also offer the functionality necessary to quickly move processes and data

---

[22] See Blazheski, *Cloud banking or banking in the clouds?* at 5 (cited in note 4); DTCC, *Moving Financial Market Infrastructure to the Cloud* at 7 (cited in note 12). Unfortunately, though the case for cloud computing being more secure than traditional data centers is compelling, there is no up-to-date empirical evidence to support the assertion because of a lack of transparency regarding reporting of vulnerabilities. See generally Ryan K.L. Ko, Stephen S.G. Lee and Veerappa Rajan, *Cloud Computing Vulnerability Incidents: A Statistical Overview*, Cloud Security Alliance (March 13, 2013).

[23] For example, one cloud service provider discovered (and alerted Intel to) significant chip-level security vulnerabilities, and the major cloud service providers all acted quickly to mitigate the vulnerability. See 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.

[24] See Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services* at 8 (cited in note 10); DTCC, *Moving Financial Market Infrastructure to the Cloud* at 6 (cited in note 12).

[25] See id.

[26] See Amazon Web Services, *AWS Best Practices for DDoS Resiliency*, 6-15 (Dec. 2018), available at https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf.

[27] See Miller, *An Introduction to Cloud Computing for Legal and Compliance Professionals* at 10 (cited in note 4).

from one cloud provider to another, increasing the resiliency of financial institutions in the event of a disruption.[28]

Data analysis and regulatory technology

As noted above, the cloud allows financial institutions to access computing resources on demand. Automatic scalability makes cloud computing uniquely suited to analysis of large data sets in real time, allowing users to log and analyze huge volumes of data on a continuous basis, rather than in discrete batches. Financial institutions can use cloud-based tools to provide richer data insights on an ongoing basis as part of their everyday operations. Cloud-based data analysis tools can also be leveraged by financial institutions and regulators both for better compliance monitoring and for a deeper understanding of risks in the financial system.

As sophisticated data analysis becomes more important for gaining competitive advantages, cloud computing is an increasingly attractive option. Major cloud providers as well as third-party intermediaries offer sophisticated data analysis software that runs on the cloud.[29] Financial institutions, as well as major cloud providers and third-party intermediaries, have developed proprietary analysis tools that run on the cloud; in fact, some financial institutions have begun to make those tools available to other, smaller institutions.[30] By giving financial institutions a real-time picture of their portfolios, these tools allow financial institutions to improve their risk management. The increasing availability of sophisticated data analysis, made possible by the use of cloud computing, not only improves the risk management of individual financial institutions—it can strengthen the health of the financial system as a whole.[31]

Cloud computing also raises new compliance possibilities for financial institutions and regulators alike. By putting better tools in the hands of financial institutions and their supervisors, cloud providers can make it easier, and more efficient, for financial institutions to comply, and for supervisors to monitor compliance, with regulatory requirements. For example,

---

[28] See generally Glen Robinson, Attila Narin, and Chris Elleman, *Using Amazon Web Services for Disaster Recovery*, Amazon Web Services (October 2014), available at http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf.

[29] See Barb Darrow, *Pssst, Amazon Cloud Is Not Really New to Banks*, Fortune (Feb. 25, 2016), available at http://fortune.com/2016/02/25/yes-banks-do-use-aws//.

[30] See Dakin Campbell, *Inside Goldman Sachs' Marquee platform* (Business Insider, Nov. 19, 2018), available at https://www.businessinsider.com/goldman-sachs-marquee-platform-2018-11.

[31] See Paul J. Davies, *New Tools Give Better Picture, Literally, of Financial-System Risk*, Wall Street Journal (April 24, 2017), *available at* https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk-1493086260?mod=article_inline; Financial Industry Regulatory Authority (FINRA), *Using the Cloud to Improve our Data Science*, available at http://technology.finra.org/articles/using-cloud-to-improve-our-data-science.html.

data analysis software running on the cloud can be used by financial institutions and regulators to better detect potential fraud or money laundering.[32] The use of cloud computing can make it feasible for regulators to increase their expectations of financial institutions: facilitating stress testing, for instance, in areas where such tests could not previously have been conducted due to data computation constraints.[33]

Andrew Haldane, chief economist of the Bank of England, famously envisioned a "global financial surveillance system" that "track[s] the global flow of funds in close to real time (from a Star Trek chair using a bank of monitors)" with "a global map of financial flows, charting spill-overs and correlations" as its centerpiece.[34] Haldane's dream may yet be a ways off, but if it or something like it comes to pass, it will likely be in part due to the widespread adoption of cloud computing by financial institutions and regulators.

c. Risks of cloud computing

While the benefits of cloud computing are significant, the use of cloud services by financial institutions also poses risks. Many of these risks are similar to the risks associated with traditional technology infrastructure, though some are unique. They range from risks associated with the technology underlying cloud computing to operational risks arising out of the relationship between financial institutions and their cloud service providers. Effective risk management requires that financial institutions understand these risks and implement a variety of technical or operational mitigations.

Technical risks

Technical risks associated with cloud computing include capacity planning failures, insecure or incomplete data deletion, and multi-tenancy and hypervisor vulnerabilities. Capacity planning – dealing with the potential for resource exhaustion – is necessary whether a financial institution uses a traditional data center arrangement or cloud services. As noted earlier, financial institutions that use proprietary data centers typically address the risk of resource exhaustion by overprovisioning, which can be very costly. Even then, they can err in estimating their needs. Financial institutions that move to the cloud effectively delegate

---

[32] See Steve Randich, *How the Cloud Is Changing Financial Regulation*, FINRA (February 17, 2016), available at http://www.finra.org/investors/how-cloud-changing-financial-regulation; Christopher Stevenson and Andrew McGuigan, *Seizing cloud opportunities: The consolidated audit trail*, Deloitte (2017), available at https://www2.deloitte.com/us/en/pages/risk/articles/the-consolidated-audit-trail-cloud-opportunities.html.
See also Financial Crimes Enforcement Network, *Treasury's FinCEN and Federal Banking Agencies Issue Joint Statement Encouraging Innovative Industry Approaches to AML Compliance* (December 03, 2018), available at https://www.fincen.gov/news/news-releases/treasurys-fincen-and-federal-banking-agencies-issue-joint-statement-encouraging.

[33] See Basel Committee on Banking Supervision, *Sound Practices: Implications of fintech developments for banks and bank supervisors*, 24 (February 2018), available at https://www.bis.org/bcbs/publ/d431.pdf.

[34] Andrew G. Haldane, *Managing global finance as a system*, Maxwell Fry Annual Global Finance Lecture, 7 (October 29, 2014), available at https://www.bis.org/review/r141030f.pdf

many of their capacity planning decisions to cloud providers. Cloud providers, for their part, must predict aggregated demand for computing resources across all their customers in order to meet the needs of their customer base. The nature of their customer base, however, gives them an advantage over managers of traditional data center environments: the demand curve of a very large, heterogeneous customer base is smoother and more predictable than the requirements for any one customer, or even several customers in one industry, because the peaks and valleys of demand of customers or market segments tend to cancel each other out.[35]

Another technical risk is insecure or incomplete data deletion. Deleting data, whether it is stored in the cloud or using traditional technology infrastructure, does not necessarily remove it entirely. In some cases, when a customer stores data in the cloud—even a single dataset—it is not stored in a single facility; to improve durability and redundancy, cloud providers may store that single object across multiple facilities. Once a financial institution deletes its data, the information is not entirely removed from the storage infrastructure. Rather the cloud provider renders the data inaccessible by anyone, and eventually reuses the underlying storage capacity. If a financial institution's data is not encrypted, that confidential data could be exposed.[36] Financial institutions can mitigate this risk by encrypting their data and subsequently deleting their encryption keys.[37]

While capacity planning failures and insecure data deletion are common to traditional platforms, cloud computing does present novel technical risks. Multi-tenancy—the ability of multiple clients to share the same physical infrastructure—is a unique feature of the cloud model. Multi-tenancy gives rise to the risk that a customer using shared infrastructure will

---

[35] Based on conversations with a major cloud service provider. See also Jim Gao, *Machine Learning Applications for Data Center Optimization* Google (2014), available at https://docs.google.com/a/google.com/viewer?url=www.google.com/about/datacenters/efficiency/internal/assets/machine-learning-applicationsfor-datacenter-optimization-finalv2.pdf; Tom Krazit, *How Amazon Web Services uses machine learning to make capacity planning decisions*, GeekWire (May 18, 2017), available at https://www.geekwire.com/2017/amazon-web-services-uses-machine-learning-make-capacity-planning-decisions/.

[36] See Lionel Dupré and Thomas Haeberlen, *Cloud Computing: Benefits, risks and recommendations for information security*, European Union Agency for Network and Information Security (ENISA), 34 (December 2012), available at https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

[37] Based on conversations with a major cloud service provider. See also 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), available at http://dx.doi.org/10.6028/NIST.IR.7956 (analyzing the additional complexity of managing cryptographic keys in cloud environments compared to enterprise IT).

expose their data or other resources to unauthorized parties.[38] Strong cloud architecture ensures that clients do not have access to data and resources that are stored on the same physical infrastructure: cloud providers strengthen the security of individual clients by virtually segregating operations using techniques for network segmentation (such as firewalls) or even micro-segmentation (which allows individual workloads to be isolated).[39]

Cloud services also depend on virtualization—the ability of multiple users to share the same physical infrastructure as if they were running their own separate machines—which relies on a software program called a "hypervisor." The hypervisor manages the multiple virtual machines that make up the cloud, allocating cloud resources to customers as needed.[40] Hypervisor vulnerabilities, which can subject it to failure or cyber-attacks, present a technical risk that may not exist in traditional technology infrastructure.[41] Cloud providers, however, have developed propriety software and hardware that reduce the vulnerability of their hypervisors to a cyber-attack. In addition, cloud providers engage in ongoing monitoring for anomalous behavior and conduct frequent penetration tests.[42]

Operational risks

Adoption of cloud computing also exposes financial institutions to operational risks, such as "lock-in" risk: the risk that a financial institution will become excessively dependent on a particular service provider.[43] Lock-in risk is not unique to the cloud: financial institutions that contract with third parties to build and maintain traditional data centers tend to enter into long-term contracts that make switching providers during the duration of the contract legally and economically costly.[44] However, financial institutions can address lock-in risk by

---

[38] See Dupré and Haeberlen, *Cloud Computing: Benefits, risks and recommendations for information security* at 29 (cited in note 36). See also Timothy Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, Carnegie Mellon University Software Engineering Institute (March 5, 2018), available at https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html/.

[39] Based on conversations with a major cloud service provider.

[40] See Donald Firesmith, *Multicore and Virtualization: An Introduction*, Carnegie Mellon University Software Engineering Institute (Aug. 14, 2017), available at https://insights.sei.cmu.edu/sei_blog/2017/08/multicore-and-virtualization-an-introduction.html.

[41] See Dupré and Haeberlen, *Cloud Computing: Benefits, risks and recommendations for information security* at 34, 37 (cited in note 36); CDW, *Protecting Financial Services Cloud Data and Applications*, 2 (2014), available at https://webobjects.cdw.com/webobjects/media/pdf/Solutions/Financial/Protecting-Financial-Services-Cloud-Data-145526.pdf.

[42] Based on conversations with a major cloud service provider.

[43] See Dupré and Haeberlen, *Cloud Computing Benefits, risks and recommendations for information security* at 17-20 (cited in note 36); Hon and Millard, *Banking in the cloud: Part 1 – banks' use of cloud services* at 11-12 (cited in note 10); Peter Bendor Samuel, *New Kind of Vendor Lock-In And Purchasing Concerns*, Forbes (Feb. 20, 2018), available at https://www.forbes.com/sites/peterbendorsamuel/2018/02/20/new-kind-of-vendor-lock-in-and-purchasing-concerns/#3ee91e8b2be6.

[44] See generally 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

operating across multiple cloud providers and by using open-source technologies, allowing them to move data and utilize services across different environments (from one cloud provider to another or from the cloud to an on-premises data center).[45] Using these strategies, financial institutions can make it easier to migrate on and off cloud providers than between bespoke managed service providers.

Since cloud services are more standardized than traditional technology platforms, they can be provided to a larger number of different clients in a more automated manner and on a larger scale, potentially increasing the concentration of financial institutions at particular cloud providers. Reliance by financial institutions on a small number of dominant cloud providers may give rise to risk, not only at the level of individual institutions, but also at the level of the financial industry as a whole.[46] To the extent that cloud computing becomes a

---

and Applications (2016), available at 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 15, 2001), available at https://sloanreview.mit.edu/article/the-hidden-costs-of-it-outsourcing/; Ian Larkin, *Bargains-then-Ripoffs: Innovation, Pricing and Lock-in in Enterprise Software*, Academy of Management Proceedings (August 2008), available at https://doi.org/10.5465/ambpp.2008.33624246.

[45] See Financial Stability Board (FSB), *FinTech and market structure in financial services: Market developments and potential financial stability implications*, 17 (Feb. 14, 2019), available at http://www.fsb.org/wp-content/uploads/P140219.pdf; Clint Boulton, *BNY Mellon, J.P. Morgan Say Cloud Foundry Prevents Vendor Lock-in*, Wall Street Journal (May 18, 2015), available at https://blogs.wsj.com/cio/2015/05/18/bny-mellon-j-p-morgan-say-cloud-foundry-prevents-vendor-lock-in/. For more on the relationship between lock-in by cloud providers and open source technology, see Ben Thompson, *Docker and the Integrated Open Source Company*, Stratechery (Dec. 9, 2014) available at https://stratechery.com/2014/docker-integrated-open-source-company/; Ben Thompson, *How Google Is Challenging AWS*, Stratechery (Nov. 30, 2016), available at https://stratechery.com/2016/how-google-cloud-platform-is-challenging-aws/; Ben Thompson, *IBM's Old Playbook*, Stratechery (Oct. 29, 2018) available at https://stratechery.com/2018/ibms-old-playbook/.

[46] See European Banking Authority, *Final Report on EBA Guidelines on outsourcing arrangements*, EBA/GL/2019/02 15 (Feb. 25, 2019), available at https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements; Financial Conduct Authority, *Guidance for firms outsourcing to the 'cloud' and other third-party IT* services, FG 16/5 7, 12, 14 (July 2018), available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf). See also Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, *Regulating and supervising the clouds: emerging prudential approaches for insurances companies*, FSI Insights on policy implementation No. 13, 4 (Dec. 2018), available at https://www.bis.org/fsi/publ/insights13.pdf; Lyndon Nelson, *Resilience and continuity in an interconnected and changing world*, Bank of England 3-4 (June 13, 2018), available at https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/resilience-and-continuity-in-an-interconnected-and-changing-world-speech-by-lyndon-nelson; Caroline Binham, *Regulator warns on European banks' reliance on cloud computing*, Financial Times (July 3, 2018), available at https://www.ft.com/content/42572d48-7ebf-11e8-8e67-1e1a0846c475; Jamie Lee, *Cyber panel flags concentration risk in cloud technology for banks, insurers*, Business Times (Oct. 2, 2018), available at https://www.businesstimes.com.sg/government-economy/cyber-panel-flags-concentration-risk-in-cloud-technology-for-banks-insurers.

part of the financial system's critical infrastructure, the industry-level risk posed by concentration of cloud providers will be of greater concern.[47] However, it is worth noting that concentration risk of this sort is not unique to cloud computing: even when using traditional, tailor-made technology infrastructures, financial institutions have historically become reliant on specific products and services, ranging from semiconductors to managed databases, many of which were produced or provided by a small number of highly dominant providers.[48]

[47] See FSB, *FinTech and market structure in financial services* at 2 (cited in note 45).

[48] See Basel Committee on Banking Supervision, *Outsourcing in Financial Services*, 18-19 (Aug. 2004), available at https://www.bis.org/publ/joint09.pdf; BITS, *BITS Guide to Concentration Risk it Outsourcing Relationships*, Financial Services Roundtable (2010), available at https://web.actuaries.ie/sites/default/files/erm-resources/bitsconcentrationrisk0910.pdf. See also Ben Thompson, *Microsoft's Monopoly Hangover*, Stratechery (July 26, 2017) available at https://stratechery.com/2017/microsofts-monopoly-hangover/ (describing the historic dominance of IT providers).

3 Existing regulatory frameworks

Financial regulators across jurisdictions have promulgated regulations and issued non-binding guidance addressing the use of cloud computing by financial institutions. These guidelines are typically based on their preexisting framework for outsourcing by financial institutions to third-party service providers. This section provides a comprehensive review of regulatory requirements and guidelines for cloud use by financial institutions in different jurisdictions, with a focus on the United States[49] and the European Union.[50]

Although they vary in their stringency and thoroughness, they share several common features. Typically, regulators identify specific risks that must be considered prior to the selection of a service provider and impose ongoing risk assessment and management obligations, including monitoring procedures and recurring audits. Financial institutions are also expected to ensure the security of data and systems in the cloud, especially sensitive customer data. Several regulators impose specific limitations on data use and processing, such as restrictions on the control, and in some cases, location, of data. Financial institutions are also generally expected to plan for contingencies, especially in the event of a service disruption or the termination of a service arrangement with a cloud provider.

---

[49] This discussion of the regulatory structure applicable to financial institutions in the U.S. in this section focuses on banking institutions. The primary statutory authority for regulating the provision of technology services to U.S. banking institutions is the Bank Service Company Act. See Bank Service Company Act, 12 USC §§ 1861–1867. The purpose of supervision under the BSCA is the monitoring of potential risks to banking institutions from their technology service providers. The U.S. federal supervisory agencies 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, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. The FFIEC sets policy regarding the responsibility of various agencies, which service providers get examined, the frequency of examination, and the scope of supervision. See generally Federal Financial Institutions Examination Council, *Supervision of Technology Service Providers*, FFIEC: IT Examination Handbook (Oct. 2012), available at https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf. It also develops examination guidelines and has established a uniform rating system for providers of technology services to banking institutions.

[50] In February 2019, the European Banking Authority (EBA) issued guidelines on outsourcing by financial institutions; these guidelines supersede both the EBA's earlier cloud-specific outsourcing guidelines and earlier general outsourcing guidelines issued by the Committee of European Banking Supervisors. See EBA, *Guidelines on outsourcing*, EBA/GL/2019/02 (Feb. 25, 2019), available at https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements. The EBA's outsourcing guidelines generally apply to all financial institutions that are within the scope of the EBA's mandate—credit institutions and investment firms subject to the Directive 2013/36/EU (Capital Requirements Directive), payment institutions and electronic money institutions—as well as their local regulators across the European Economic Area. The aim of the outsourcing guidelines is to establish a common framework for outsourcing by financial institutions across Europe, thereby ensuring a more level playing field for different types of financial institutions.

Regulatory expectations typically vary based on the relative importance or materiality of functions that are moved to the cloud. The European Banking Authority (EBA), for example, applies stricter criteria where financial institutions outsource critical or important functions that have a strong impact on their risk profile or internal control framework.[51] Supervisory agencies in the United States also impose more stringent obligations when banks outsource critical activities to third-party service providers, including cloud providers.[52] Whether particular functions are important or material is not always well-specified in regulations or other guidance; in general, regulators look to whether the activity relates to a financial institution's core business operations and whether its failure would materially impair its regulatory obligations, financial performance, or its ability to continue its business activities.[53]

a. Outsourcing prerequisites

Though the prerequisites for adopting cloud services differ across jurisdictions, common themes include a requirement or recommendation that financial institutions undertake a preliminary risk assessment of the cloud service provider and the particular services to be adopted. In addition, regulators often require that financial institutions notify, or obtain approval from, regulators before outsourcing to a cloud service provider—especially when the outsourcing relates to material or important functions.

Due diligence

Outsourcing guidelines published by the Federal Financial Institutions Examination Council (FFIEC),[54] an interagency body comprising the various U.S. bank regulators, provide that a

---

[51] See EBA, *Guidelines on outsourcing*, Section 4 (cited in note 50).

[52] See, for example, Office of the Comptroller of the Currency, *Risk Management Guidance*, OCC Bulletin, 2013-29, available at https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html ("The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is necessary when a third-party relationship involves critical activities.").

[53] See, for example, EBA, *Guidelines on outsourcing*, Section 4, par. 29 (cited in note 50).

[54] The FFIEC publishes principles-based guidance to assist regulators and financial institutions in evaluating a financial institution's IT risk management processes in the form of IT Handbooks, one of which provides guidance for banking institutions' responsibilities to establish, manage, and monitor information technology outsourcing, including the use of cloud services. See Federal Financial Institutions Examination Council (FFIEC), *Outsourcing Technology Services*, FFIEC: IT Examination Handbook (June 2004), available at https://ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf. In 2012, the FFIEC issued an informational notice regarding what it viewed as the key elements of outsourced cloud computing implementation and risk management. The 2012 notice emphasizes that cloud computing should be considered "another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing." See FFIEC, *Outsourced Cloud Computing*, 1 (July 10, 2012), available at https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf. Several of the FFIEC member agencies have issued their own guidance for managing third-party outsourcing relationships, including with technology service providers. See, for example, Federal Reserve Board, *Guidance on Managing Outsourcing Risk*, Division of Banking Supervision and Regulation Division of Consumer and Community Affairs Board of Governors of the

banking institution should perform due diligence on a service provider in order to ensure that the service provider meets the institution's needs.[55] In its separate informational notice on cloud computing, the FFIEC recommends that, prior to choosing a cloud service provider, a banking institution perform due diligence to ensure that potential cloud service providers will meet the institution's requirements for cost, quality of service, compliance with regulatory requirements and risk management.[56] Similarly, the EBA outsourcing guidelines direct a financial institution to conduct a thorough risk assessment with respect to the outsourced activities and undertake due diligence to ensure that the service provider is suitable.[57] This risk assessment process should include deciding on an appropriate level of data confidentiality, service continuity and data and system integrity (as well as consideration of specific measures necessary for data security, such as the use of encryption).[58]

Guidance published by some regulators includes diligence items that are specific to cloud outsourcing.[59] The Monetary Authority of Singapore's outsourcing guidelines, for example, provide that financial institutions should ensure that cloud service providers possess the ability to identify and segregate user data using strong physical or logical controls and have robust access controls in place to protect customer information.[60] The IT capabilities of cloud providers are also a focus of some outsourcing guidelines: guidance published by the

---

Federal Reserve System (Dec. 5, 2013), available at https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf (general outsourcing); Federal Deposit Insurance Corporation, *Guidance for Managing Third-Party Risk*, FIL-44-2008 (June 6, 2008), available at https://www.fdic.gov/news/news/financial/2008/fil08044.html (general outsourcing); Federal Deposit Insurance Corporation, *Financial Institution Letter Re: Bank Technology Bulletin*, FIL-50-2001 (June 4, 2001), available at https://www.fdic.gov/news/news/financial/2001/fil0150.html (technology outsourcing); Office of the Comptroller of the Currency, *Risk Management Guidance*, OCC Bulletin, 2013-29, available at https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (general outsourcing).

[55] See FFIEC, *Outsourcing Technology Services* at 10-11 (cited in note 54).

[56] See FFIEC, *Outsourced Cloud Computing* at 2 (cited in note 54).

[57] See EBA, *Guidelines on outsourcing*, Sections 12.2, 12.3 (cited in note 50).

[58] See id at 12.2(e).

[59] See, for example, Australian Prudential Regulation Authority (APRA), *Outsourcing Involving Cloud Computing Services*, 12-13 (Sept. 24, 2018), available at https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf.

[60] See Monetary Authority of Singapore (MAS), *Guidelines on Outsourcing*, Section 6.7 (Oct. 2018). MAS's guidelines apply to banks, insurers, financial adviser, certain participants in capital markets, and payment and settlement systems companies.

Financial Conduct Authority (FCA), the United Kingdom's financial regulator, advises financial institutions to take into account a cloud service provider's adherence to international IT standards.[61]

Regulatory notice and approval

The FFIEC outsourcing guidelines do not specifically require any regulatory involvement before a banking institution moves its activities to the cloud.[62] The EBA guidelines, on the other hand, provide that financial institutions should inform their respective regulatory authorities in a timely manner or engage in supervisory dialogue with competent authorities regarding planned outsourcing of critical or important functions (or where a previously outsourced function becomes critical or important).[63]

Other jurisdictions require regulatory approval for certain kinds of cloud outsourcing. South Korea requires financial institutions to provide the Financial Supervisory Service with a detailed report prior to using the cloud for significant activities, including those that involve unique identifiable information or personal credit information or that otherwise significantly affect the safety and reliability of electronic financial transactions. If regulators deem the due diligence, business continuity plan or security measures undertaken by the financial institution to be inadequate, they can require improvement or supplementation of the report prior to approval.[64] The central bank of the Philippines requires banking institutions

---

[61] See Financial Conduct Authority (FCA), *Finalised guidance: FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services*, 7 (July 2018), available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf. The FCA's guidance no longer applies to banks or investment firms to whom the EBA guidelines are addressed, but they still apply to all other financial services firms (including banks, credit unions and insurance firms), consumer credit firms, investment firms (including asset managers, wholesale investment firms, retail investment firms, insurance intermediaries and mortgage brokers), benchmark administrators and some payment services and e-money firms.

[62] Under the Bank Service Company Act, however, banks are required to notify their primary supervisor of the existence of certain outsourcing relationships within 30 days of the start of the relationship. See 12 USC § 1867(c)(2). Federal savings associations are subject to similar requirements set forth in 12 USC § 1464(d)(7)(D)(ii) and 12 USC § 1867(c)(2). Federal regulatory agencies have implemented this notification requirement in a variety of different ways. The FDIC, for example, has developed a form for FDIC-supervised banks on which to report the necessary information. See FDIC, *Financial Institution Letter Re: Required Notification for Compliance with the Bank Service Company Act* (cited in note 54).The OCC, by contrast, requires banks to maintain a current inventory of all outsourcing relationships that is available to examiners upon request. See OCC, *Description Risk Management Guidance* (cited in note 54).

[63] See EBA, *Guidelines on outsourcing*, Section 11, par. 58 (cited in note 50). Other regulators require notification for certain kinds of cloud outsourcing: banks in India, for example, are required to report significant cloud outsourcing arrangements if data is shared across geographic locations. See Reserve Bank of India, *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds* (April 2011), available at https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

[64] See Financial Services Commission (FSC)*, Regulation on Supervision of Electronic Financial Transactions*, Notice No. 2018-36, Article 14-2 (amended Dec. 21, 2018). South Korea's cloud outsourcing requirements are broadly

that it considers riskier to get approval before outsourcing systems or processes to the cloud. Approval is granted based on an assessment of the bank's ability to manage the risks associated with cloud outsourcing. Banks that the central bank deems to be safer can outsource to the cloud without prior approval.[65]

b. Ongoing obligations

Mandatory risk assessment and management continues after a financial institution enters into a cloud services agreement. Regulators mandate that the financial institution monitor the cloud service provider, including by engaging in regular audits and obtaining reporting from the provider, as long as the financial institution uses its services. Many regulators also demand that the financial institution obtain certain information and access rights from its cloud service provider, either for the financial institution, its supervisory regulator, or both.

Monitoring and control

Regulators typically require that individual financial institutions monitor their cloud service providers on an ongoing basis. For example, the FFIEC's outsourcing guidelines provide that banking institutions should monitor their service providers performance on an ongoing basis, with an emphasis on the service provider's security controls, financial strength, and the effects of any external events.[66] The FFIEC's notice on cloud computing focuses on monitoring security-related threats, incidents and events affecting both a banking institution's own and its cloud provider's networks.[67] The statement also emphasizes that, for high-risk activities, "continuous monitoring may be necessary for [banking] institutions to have a sufficient level of assurance that the servicer is maintaining effective controls." [68] The EBA guidelines likewise provide that financial institutions should review and monitor the performance of service providers on an ongoing basis using a risk-based approach, with a focus on critical or important functions and ensuring the availability, integrity and security of data and information.[69]

Other regulators require that financial institutions take specific organizational measures as part of their ongoing oversight of service providers, including cloud providers. The Swiss Financial Market Supervisory Authority (FINMA), for example, mandates that, as part of its

---

applicable across the financial industry: they apply to banks, insurance companies, financial investment entities, specialized credit finance entities and savings banks, as well as electronic financial business entities.

[65] See Bankgo Sentral ng Pilipinas, *Amendment to the Guidelines on Outsourcing*, Circular No. 899: Series of 2016 (Jan. 18, 2016), available at http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf.

[66] See FFIEC, *Outsourcing Technology Services* at 18-19 (cited in note 54).

[67] See FFIEC, *Outsourced Cloud Computing* at 2 (cited in note 54). The notice suggests that additional controls may be required if a cloud service provider is unfamiliar with the financial industry and relevant legal and regulatory requirements

[68] See id at 3.

[69] See EBA, *Guidelines on outsourcing*, Section 14 (cited in note 50).

ongoing monitoring of a service provider, a financial institution designate a unit that is responsible for monitoring and controlling the provider and ensure that its service agreement with the provider gives it the necessary rights for instruction and control.[70] Similarly, guidelines published by the Monetary Authority of Singapore provide that financial institutions should establish a structure to manage and control their outsourcing arrangements with services providers and lists several baseline measures (including creating reporting policies and procedures, and conducting annual reviews) that financial institutions should follow to ensure that service providers uphold performance, operational, internal control and risk management standards on an ongoing basis.[71]

Audits

As part of its ongoing risk assessment and management responsibilities, financial institutions generally are required to audit their cloud service providers. Regulators differ with respect to the extent to which institutions can rely on audits and certifications performed by or for the cloud service provider. While some jurisdictions require that audits of cloud service providers be performed by a financial institution's internal or external auditors, others allow financial institutions to rely solely on a cloud service provider's external auditor or internal audit department—as long as the auditor complies with certain regulatory standards.[72]

The FFIEC's notice on cloud computing recommends that banking institutions make use of auditors to evaluate the adequacy of cloud service providers' internal controls, and in particular, notes that the assistance of third-party auditors with expertise in evaluating cloud environments may be necessary.[73] Several regulators, including the EBA, authorize community audits organized by a group of financial institutions that appoint a lead auditor from one of the institutions or an independent third-party auditor on their behalf.[74] Community audits are recognized as a means of using audit resources more efficiently and reducing the organizational burden on both participating financial institutions and the service provider.

---

[70] See Swiss Financial Market Supervisory Authority (FINMA), *Outsourcing – banks and insurers*, Circular 2018/3, 4-5 (September 21, 2017), available at https://www.finma.ch/en/news/2017/12/20171205-mm-rs-outsourcing/. FINMA's outsourcing circular applies to banks, insurers and securities dealers.

[71] See MAS, *Guidelines on Outsourcing*, 5.8.2 (cited in note 60).

[72] See, for example, id, Section 5.9.6. The EBA allows financial institutions to rely on third-party certifications and reports in the case of outsourcing of functions that are not critical or important. The EBA guidelines emphasize that in the case of cloud outsourcing, financial institutions should verify that whoever is performing the audit has appropriate qualifications. EBA, *Guidelines on outsourcing*, Section 13.3, pars. 91-93, 97 (cited in note 50).

[73] See FFIEC, *Outsourcing Cloud Computing* at 3 (cited in note 54).

[74] See EBA, *Guidelines on outsourcing*, Section 13.3, par. 91(a) (cited in note 50); Federal Financial Supervisory Authority (BaFin), *Cloud computing: Compliance with the supervisory requirements regarding rights of information and audit and ability to monitor*, BaFin Journal (May 7, 2018), available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1804_Cloud_Computing_en.html.

In these cases, regulators typically specify that audit reports should be based on generally recognized auditing standards and be performed by auditors with adequate expertise.[75]

Information and access rights

An important factor in facilitating effective monitoring is securing the right to certain information and access; regulators generally expect that certain basic information and access rights will be included in a financial institution's cloud services contract, but differ as to the required scope of those rights—what must be accessed by financial institutions and their regulatory supervisors. The FFIEC's outsourcing guidelines provide that a banking institution's outsourcing contract should, among other things, specify the rights of the institution and its regulatory agencies to obtain the results of audits in a timely manner. In the case of Internet-related services, the FFIEC guidelines recommend sufficiently detailed reports on the findings of ongoing audits to adequately assess security without compromising the service provider's security.[76]

The EBA outsourcing guidelines go further, requiring that financial institutions secure from service providers (including cloud providers) both a right to audit as well as a right of physical access to the service providers' relevant business premises. Such access and audit rights are required for both the institutions themselves as well as their regulatory supervisors with respect to any outsourcing of critical or important functions.[77] Several other regulators—like the EBA—require that financial institutions secure audit rights for themselves and their supervisors that include access to the premises of cloud service providers. For example, the Australian Prudential Regulation Authority (APRA) mandates that a financial institution that outsources a material business activity to a cloud service provider must ensure that the provider makes available to APRA information and documents upon request and allows APRA to conduct onsite visits at the provider.[78]

---

[75] See EBA, *Guidelines on outsourcing*, Section 13.3, par. 90 (cited in note 50); BaFin, *Cloud computing: Compliance with the supervisory requirements regarding rights of information and audit and ability to monitor* (cited in note 74).

[76] See FFIEC, *Outsourcing Technology Services* at 13 (cited in note 54).

[77] See EBA, *Guidelines on outsourcing*, Section 13.3, par. 87 (cited in note 50). Audit and access requirements for functions that are not critical or important should follow a risk-based approach based on the nature of the outsourced function and its associated risks. See id at par. 88. Prior to the EBA issuing guidelines on outsourcing, outsourcing guidelines issued in December 2006 by the Committee of European Banking Supervision (a predecessor to the EBA) required audit rights for European regulators. A number of European national regulators, such as the Dutch National Bank (DNB) and the U.K. FCA, had also issued more detailed guidance on requirements for audit rights, including requiring audit rights for the financial institutions. See, for example, De Nederlandsche Bank N.V., *Circulaire Cloud Computing: English Final* (January 10, 2012). DNB's cloud circular applied to settlement institutions, payment services providers, clearing institutions, electronic money institutions, and banks.

[78] See APRA, *Prudential Standard CPS 231: Outsourcing*, par. 34 (July 2017), available at https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.

Regulators do recognize practical limits on their information and audit rights: APRA, for example, will in the normal course seek to obtain information that it needs from financial institutions first before requesting information directly from cloud service providers.[79] In a similar vein, cloud guidance published by the U.K. FCA clarifies that, although access to a cloud provider's "business premises" may be required, access to some sites—including data centers—may be limited for legitimate security reasons.[80]

Hong Kong's outsourcing guidelines focus on ensuring that access to data by regulators and the bank's internal and external auditors is not impeded by the use of outsourced services.[81] To that end, financial institutions are required to ensure that their outsourcing agreements allow for supervisory inspections or review of operations of service providers as they relate to outsourced activities. In addition, financial institutions should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by regulators and that any data retrieved from third-party service providers are accurate and available in Hong Kong on a timely basis.[82] Japan's computer security guidelines for financial institutions, published by the Center for Financial Industry Information Systems (FISC), mandate the inclusion of several contract provisions relating to ongoing oversight, such as provisions requiring cloud providers to disclose information to a financial institution in the event of increased risk of information leakage or in the event the cloud provider's internal controls have weakened.[83]

c. Security of data and systems

Beyond the procedural requirements associated with performing adequate due diligence and ongoing monitoring of financial institutions' cloud service providers, regulators also set substantive requirements regarding the security of financial institutions' data in the cloud.

Security and confidentiality

Regulators place significant emphasis on the security of financial institutions' cloud activities, typically requiring that they ensure that their cloud service providers maintain robust

---

[79] See id.

[80] See FCA, *Finalised guidance: FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services* at 11 (cited in note 61).

[81] See Hong Kong Monetary Authority (HKMA), *Supervisory Policy Manual: Outsourcing*, Section 2.8 (Dec. 28, 2001), available at https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.

[82] See id, Section 2.8.1.

[83] See Center for Financial Industry Information Systems (FISC), *Security Guidelines on Computer Systems for Financial Institutions*, Section V-2(1) No. 21 (9th Edition, 2018). The FISC guidelines take a risk-based approach, according to which the appropriateness of particular contractual provisions depends in part on the nature of the workload that they are outsourcing. See also id, Section V-2(2) No.24, which details ongoing monitoring requirements that are specific to cloud services.

security measures and comprehensive security policies.[84] The FFIEC outsourcing guidelines require that banking institutions ensure that their service providers' physical and data security standards are sufficient to meet their legal and commercial requirements and that outsourcing agreements specifically address a service provider's responsibility for security and confidentiality of a banking institution's data and other resources.[85] In addition, the FFIEC's notice on cloud computing recommends that banking institutions verify their cloud service providers data handling procedures, what controls the cloud service provider has to ensure the integrity and confidentiality of the banking institution's data, and the adequacy and availability of backup data. The statement also provides specific recommendations with respect to monitoring of security-related threats to the institution's and its servicers' networks as well as data deletion and removal.[86] The EBA outsourcing guidelines, like the FFIEC's, require that financial institutions ensure that service providers comply with appropriate IT security standards, and that data and system security requirements are defined within the outsourcing agreement and monitored for compliance.[87]

Other jurisdictions impose more specific requirements with respect to the security of a financial institution's data when using outsourced services of any kind, especially with respect to confidential personal information. The Hong Kong Monetary Authority, for example, has published technology guidelines that include detailed principles for security management designed to ensure the integrity and confidentiality of customer data.[88] The Monetary Authority of Singapore's outsourcing guidelines require that a financial institution and service provider explicitly allocate, in their contract, the responsibilities of parties with respect to security and liability for losses in the event of a breach of security or confidentiality that results in the disclosure of customer information.[89]

---

[84] See, for example, APRA, *Outsourcing Involving Cloud Computing Services* at 12-13 (cited in note 59) (requiring that financial institutions take into account the ability of a cloud service provider to meet security requirements and have secure design principles and development practices); Office of the Superintendent of Financial Institutions (Canada), *Outsourcing of Business Activities, Functions and Processes*, Section 7.2.1(j) (Dec. 2003) (mandating appropriate security and data confidentiality protections and requiring that service providers be able to logically isolate a financial institution's data, records, and items in process from those of other clients at all times, including under adverse conditions) (March 2009).

[85] See FFIEC, *Outsourcing Technology Services* at 12, 26 (cited in note 54).

[86] See FFIEC, *Outsourced Cloud Computing* at 3-4 (cited in note 54).

[87] See EBA, *Guidelines on outsourcing*, Section 13.2 (cited in note 50).

[88] See HKMA, *Supervisory Policy Manual: General Principles for Technology Risk Management*, TM-G-1, Section 3 (June 24, 2003), available at https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf.

[89] See MAS, *Guidelines on Outsourcing*, Section 5.6.2(a) (cited in note 60).

Regulators also expect financial institutions to take their privacy obligations into account, and in some cases require that they maintain higher levels of security with respect to personal data in order to safeguard the privacy and confidentiality their customers.[90] The FFIEC outsourcing guidelines require banking institutions to ensure that service providers have appropriate measures in place to comply with applicable laws and supervisory expectations governing the confidentiality of customer information.[91] In the European context, both financial institutions and cloud service providers are subject to the General Data Protection Regulation (GDPR).[92] The EBA outsourcing guidelines mandate a risk-based approach to ensuring that sensitive data is adequately protected and kept confidential. In particular, financial institutions are required to take into account differences between privacy regimes in different jurisdictions, especially in connection with the requirements imposed by the GDPR.[93]

The GDPR, which imposes restrictions on the storage and use of personal data, is one of several non-financial sector specific data protection frameworks imposed on financial institutions and cloud service providers.[94] India, for instance, has a comprehensive framework for regulating information technology that imposes data protection requirements (and potential liability) on the handling of personal information, including by financial institutions and cloud service providers.[95] These comprehensive data protection regimes, which are not specific to the financial sector, are beyond the scope of this report.

Limits on data use and storage

Several jurisdictions also impose specific limits on how a financial institution's data can be used by a cloud service provider and how it must be stored. The FFIEC outsourcing guidelines mandate that agreements with service providers forbid the service provider from using or disclosing a banking institution's information, except as necessary to or consistent with provision of the relevant services, and to protect against unauthorized use.[96] Although it does not include any specific restrictions on data storage or use, the FFIEC's notice on cloud computing recommends that, before transferring data to a cloud service provider, banking

---

[90] See, for example, Financial Security Institute (South Korea), *FSI Guidelines on Use of Cloud Services in the Financial Industry*, 15 (January 2019) (providing that systems that process unique identifiable information or personal credit information cannot be designated as "less-significant" information processing systems subject to less stringent regulatory requirements).

[91] See FFIEC, *Outsourcing Technology Services* at 26 (cited in note 54).

[92] Regulation (EU) 2016/679, L119/1 (May 4, 2016).

[93] See EBA, *Guidelines on outsourcing*, Section 13.2, pars. 83-84 (cited in note 50).

[94] Banking institutions in the United States, by contrast, are only subject to financial-sector specific privacy requirements under the Graham-Leach-Bliley Act. See 15 USC §§ 6801–6809.

[95] See generally The Information Technology (Amendment) Act, 2008, Feb. 5, 2009/Magha 16, 1930 (Saka); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, GSR 313(E) (April 11, 2011).

[96] See FFIEC, *Outsourcing Technology Services* at 12 (cited in note 54).

institutions understand how its data will be stored and used—in particular, whether its data will share resources with data from other cloud clients, (such as whether it will be transmitted over the same networks, and stored or processed on servers that are also used by other clients).[97]

The EBA outsourcing guidelines do not impose any specific measures regarding the storage and usage of data, but they do require financial institutions to consider whether such measures are required for the protection of data. The guidelines also mandate that financial institutions include in outsourcing contracts for critical or important functions provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data.[98]

Similar to the FFIEC outsourcing guidelines, regulators typically require that financial institutions ensure that a service provider, such as a cloud provider, is not able to use the financial institution's data for any purpose other than that which is necessary to provide services.[99] Other regulators impose additional requirements regarding data processing and storage, such as a requirement that a financial institution's data is segregated from all other data held by the cloud service provider: the Monetary Authority of Singapore, for example, mandates that financial institutions ensure that cloud providers clearly identify and segregate customer data using "strong physical or logical controls" in order to protect customer information.[100]

d. Data residency requirements

Several jurisdictions impose restrictions on cross-border cloud outsourcing—limiting where data transferred to a cloud service provider can be stored and processed. Regulators identify several concerns that motivate data residency requirements, including: (1) whether standards for security and resiliency in the cloud provider's home jurisdiction are satisfactory; (3) whether data located outside the financial institution's home jurisdiction will continue to be accessible to regulators in that jurisdiction; and (3) whether privacy rules in the cloud provider's home jurisdiction adequately protect customers.[101] This section reviews existing data residency requirements and other limitations on cross-border outsourcing, but does not take a position as to whether they are necessary or sufficient to address these concerns. More broadly, this section does not include an evaluation of the potential costs and consequences of these limitations.

---

[97] See FFIEC, *Outsourced Cloud Computing* at 2 (cited in note 54).
[98] See EBA, *Guidelines on outsourcing*, Section 12.2, par. 68(e); Section 13, par. 75(g) (cited in note 50).
[99] See, for example, HKMA, *Supervisory Policy Manual: Outsourcing*, Section 2.5 (cited in note 81) (data should not be used for any purpose by a service provider without the consent of the financial institution and should comply with relevant privacy rules).
[100] See MAS, *Guidelines on Outsourcing*, Section 6.7 (cited in note 60).
[101] See, for example, EBA, *Guidelines on outsourcing*, Section 13.2, pars. 83-84; Title V, par. 119 (cited in note 50).

The FFIEC's notice on cloud computing does not restrict the transfer of data on the cloud to other jurisdictions, but notes that a banking institution should understand the applicability of laws within a host country and the banking institution's ability to control access to its data.[102] The EBA outsourcing guidelines likewise allow for data to be transferred to different jurisdictions. However, they require financial institutions to adopt a risk-based approach to data storage and processing locations and to take into account differences between jurisdictions regarding the protection of data.[103] The outsourcing guidelines also require regulatory authorities to ensure that they are able to perform effective supervision, in particular when institutions outsource critical or important functions outside the E.U./European Economic Area.[104]

Guidelines published by the U.K. FCA similarly recommend that financial institutions ensure that data is not stored in jurisdictions that may inhibit effective access to such data for U.K. regulators. Considerations identified by the FCA as important include the wider political and security stability of the jurisdiction; the law in force in the jurisdiction in question (including data protection); and the international obligations of the jurisdiction.[105]

Other jurisdictions require that financial institutions notify their customers and/or consult with regulators before transferring data to another jurisdiction. Hong Kong's outsourcing guidelines require that financial institutions give notice to customers of significant outsourcing activities, particularly where such outsourcing is outside of Hong Kong.[106] Australia mandates that financial institutions consult with its prudential regulator before using cloud services in another jurisdiction, to ensure that the financial institution's due diligence process adequately addresses the effect of the cross-border arrangement on the institution's risk management framework.[107]

Some jurisdictions prohibit the transfer of certain data outside the financial institution's home jurisdiction outright. In China, financial institutions are prohibited from transferring personal financial data outside China; storage, processing and analysis of personal financial information must be conducted within China.[108] Other regulators allow the cross-border

---

[102] See FFIEC, *Outsourced Cloud Computing* at 4 (cited in note 54).

[103] See EBA, *Guidelines on outsourcing*, Section 13.2, pars. 83-84; Section 12.1, par. 68 (cited in note 50).

[104] See id, Title V, par. 119.

[105] See FCA, *Finalised guidance: FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services* at 9 (cited in note 61).

[106] See HKMA, *Supervisory Policy Manual: Outsourcing*, Section 2.5.3 (cited in note 81).

[107] See APRA, *Prudential Standard CPS 231: Outsourcing*, par. 39 (cited in note 78). APRA also expects financial institutions to consider Australian-hosted options as they evaluate cloud service offerings, noting that (at least according to APRA), Australian hosting can mitigate risks that might impede a financial institution's ability to meet its obligations or APRA's ability exercise its role as a prudential regulator. See APRA, *Outsourcing Involving Cloud Computing Services* at 12 (cited in note 59).

[108] See People's Bank of China, *Notice Requesting Financial Institutions to Properly Conduct Personal Financial Information, Circular 17* (Jan. 21, 2011).

transfer of data, but only subject to specific requirements. Switzerland's FINMA, for example, not only stipulates that data can only be transferred outside Switzerland if FINMA retains its right to audit the cloud service provider, but also requires that all information that could be needed for restructuring or resolution of the financial institution be accessible from Switzerland.[109] Chile's supervisory authority does not require that all of a financial institution's data be stored within Chile; however, it mandates that financial institutions that outsource strategic or material activities abroad maintain a local data center in Chile for contingency purposes.[110]

e. Business continuity and contingency planning

In order to ensure the reliability of the cloud services used by financial institutions, regulators require that financial institutions put in place business continuity plans dealing with service disruptions and other contingencies.[111] An important aspect of contingency planning by financial institutions involves the ability of those financial institutions to terminate their service relationship with a cloud provider without disrupting any material functions.[112]

Operational resiliency

Recognizing that service disruptions can have significant impacts on a financial institution's operations, as well as on the broader financial system, regulators require that financial institutions monitor their cloud service providers' resilience and plan for potential service disruptions. The cloud computing notice published by the FFIEC indicates that a banking institution's disaster recovery and business continuity plans should include appropriate consideration of the nature of cloud computing, the cloud provider's disaster recovery and business continuity plans, as well as the availability of essential communications links.[113] The EBA outsourcing guidelines require financial institutions to plan and implement arrangements to maintain their ongoing functions in the event that services provided by a cloud provider fail or deteriorate to an unacceptable degree.[114] They also entitle a financial institution's

---

[109] See FINMA, *Outsourcing – banks and insurers* at 5-6 (cited in note 70).

[110] See Superintendencia de Bancos e Instituciones Financieras (SBIF), *Recopilación Actualizada de Normas (Updated Compilation of Regulations)*, Chapter 20-7, Section IV(1)(b). The SBIF recently proposed allowing financial institutions to forego a local data center, provided the financial institution's outsourcing arrangement meets certain availability and recovery time objectives. See SBIF, *SBIF publica para comentarios modificaciones a normas sobre externalización de servicios* (May 27, 2019), available at https://www.sbif.cl/sbifweb/servlet/Noticia?indice=2.1&idContenido=12523. In June 2019, the SBIF was merged into the Comisión para el Mercado Financiero, which is responsible for oversight of securities markets, insurance, banks and other financial institutions.

[111] See W. Kuan Hon and Christopher Millard, *Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing'*, 34 Computer Law & Sec. Rev. 337, 353-54 (2018).

[112] See id at 354.

[113] See FFIEC, *Outsourced Cloud Computing* at 2 (cited in note 54).

[114] See EBA, *Guidelines on outsourcing*, Section 9 (cited in note 50).

supervising regulator to ask for additional information on the financial institution's risk analysis for critical or important outsourced activities, such as whether the provider has a service continuity plan that is suitable for the service provided to the financial institution.[115]

Several other regulators often require financial institutions to set specific resiliency targets in their outsourcing agreements. Guidance published by Switzerland's FINMA, for example, requires that a financial institution and cloud service provider draw up a security framework to ensure the continuity of the functions that are outsourced to the cloud in case of an emergency, but does not provide specific service availability, recovery and resumption objectives.[116] Likewise, the Monetary Authority of Singapore's outsourcing guidelines requires financial institutions to include in their outsourcing agreements specific recovery objectives and to periodically test its disruption preparedness with its service providers. Notably, standards for business continuity depend on the importance of the financial institution – when interdependency on an institution in the financial system is high, the Monetary Authority of Singapore imposes higher preparedness standards.[117] However, regulators generally do not impose definite availability and recovery requirements—for example, that in the event of a disruption, that service must be restored within a particular amount of time—on most financial institutions.[118]

Exit strategies

Another aspect of contingency planning involves the ability of financial institutions to terminate their service relationship with a cloud provider. Developing an exit strategy is particularly important in addressing lock-in risk, to ensure that financial institutions can transition from an outsourced service provider as needed for commercial or technical reasons. Regulators typically require that financial institutions have exit provisions in outsourcing contracts that, among other things, require service providers to work with financial institutions to return their data.[119] These mandatory exit provisions generally also require that service providers delete all of a financial institution's data from their systems.[120]

---

[115] See id, Title V, par. 112.

[116] See FINMA, *Outsourcing – banks and insurers* at 5 (cited in note 70).

[117] See MAS, *Guidelines on Outsourcing*, Section 5.7 (cited in note 60).

[118] But see CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, Section 6.2.2 (June 2016), available at https://www.bis.org/cpmi/publ/d146.pdf (providing that providers of financial market infrastructure—such as a systemically important payment system, central securities depositary, securities settlement system, central counterparty or trade repository—should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption).

[119] See, for example, MAS, *Guidelines on Outsourcing*, Section 5.5.2(i) (cited in note 60). See also Hon and Millard, *Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing'* at 354 (cited in note 111).

[120] See, for example, HKMA, *Supervisory Policy Manual: Outsourcing*, Section 2.5.4 (cited in note 81) (in the event of termination, financial institutions should ensure that all data is retrieved from a service provider or destroyed).

The FFIEC's notice on cloud computing, for example, recommends that cloud service contracts provide clarity with respect to disengagement of a cloud provider and specify that data can be removed from all locations where it is stored on the cloud provider's network.[121] The EBA outsourcing guidelines provide that a financial institution should make sure that it can exit a service arrangement, if needed, without disrupting provision of services and without being detrimental to the continuity of its services.[122] To that end, the guidelines require that outsourcing financial institutions develop and test comprehensive exit plans and identify alternative solutions to enable them to remove outsourced functions and data from a service provider and transfer them to alternative providers or back to the institution.[123] They also mandate that outsourcing agreements include an obligation for service providers to support, in the event of termination, a financial institution in the transfer of activity, data or services to another service provider or back to the institution.[124]

Guidelines published by Japan's FISC provide detailed, specific requirements regarding termination of cloud services.[125] They provide that outsourcing contracts must address exit procedures and responsibilities, by including provisions requiring the cloud provider to facilitate the extraction of data that will be transferred to a new cloud provider or an existing in-house system and allocating the burden of transfer expenses in different scenarios.[126] The guidelines also include instructions for protecting data upon termination, mandating that: data provided by financial institutions be erased in an appropriate manner and time frame; information linking the data management area and data storage area be severed; and that the data storage area be wiped.[127]

---

[121] See FFIEC, *Outsourced Cloud Computing* at 3-4 (cited in note 54).
[122] See EBA, *Guidelines on outsourcing*, Section 7, par. 42; Section 15 (cited in note 50).
[123] See id.
[124] See id, Section 13.4.
[125] See FISC, *Security Guidelines on Computer Systems for Financial Institutions*, Section V-2(1) No. 21 (cited in note 83).
[126] See id.
[127] See id.

4 Facilitating cloud adoption in the financial sector

The benefits of cloud computing are largely a result of its singular technological and business model: a utility-like model in which computing resources are shared by a cloud provider's many users, who can automatically scale up their usage when additional resources are needed and reduce it when those needs subside. Regulatory frameworks developed in the context of traditional third-party outsourcing, however, contemplate a one-to-one provider-to-customer relationship typical of legacy technology infrastructure like on-premises data centers.

This traditional framework is ill-suited to the cloud model, which makes the adoption of cloud by financial institutions more difficult. For one, the traditional model places the onus of assessing and managing risk on individual financial institutions. In the context of cloud computing, however, that model is inefficient: it requires financial institutions to monitor the same infrastructure that is used by multiple clients, and monitoring by the marginal financial institution does little to increase overall cloud security. Moreover, requiring financial institutions to individually monitor a cloud provider can actually increase security risks to the cloud provider and potentially to other customers' cloud environments; auditing by an individual financial institution can require access to the cloud provider in a manner that exposes the information of one financial institution to another. Finally, individual financial institutions are not well-suited to identifying risks to multiple financial institutions from utilizing the same cloud provider.

Also, unlike traditional technology infrastructure, which can be built and operated to the regulatory specifications of an individual financial institution, cloud infrastructure can be used by thousands, if not millions, of customers located across multiple jurisdictions—each subject to its own regulatory requirements. The cross-border nature of cloud services, which involve the provision of computing resources to millions of clients located in many different jurisdictions and subject to an array of disparate regulatory regimes, raises a set of issues that might not apply in the traditional outsourcing context.

The U.S. Treasury Department has recommended that federal regulators ease the adoption of new technologies such as cloud computing, with the aim of reducing barriers to the migration of activities to the cloud.[128] Specific regulatory actions recommended by Treasury include clarifying how audit requirements may be met in the cloud.[129] Treasury has also recommended the formation of a cloud and financial services working group among financial regulators that would engage industry stakeholders, including cloud service providers, financial institutions, and others in order to develop more informed policies regarding the use of cloud computing by financial institutions.[130] Clarifying expectations for audits of cloud services and enhancing collaboration between regulators are important steps that can

[128] See Mnuchin and Phillips, *U.S. Treasury Report* at 44-52 (cited in note 7).
[129] See id at 51.
[130] See id at 52.

be taken to ensure the safety of cloud services and facilitate the migration of activities to the cloud by financial institutions. In addition, regulators should continue to engage in a risk-based dialogue on potential industry-level issues posed by cloud adoption, which should increase understanding of and comfort with more widespread cloud use by financial institutions.

Community audits

Independent audits of cloud providers are fundamental to ensuring that cloud services are secure and resilient. The existing requirements imposed on financial institutions that adopt cloud services – ranging from the security of data and systems to operational resiliency – depend in part on protections in place at the cloud provider. Audits are therefore a critical part of both due diligence and monitoring. Presently, with limited exceptions, regulatory guidance generally expects that each financial institution conduct its own audit of the cloud provider—even when the same cloud provider offers services to other financial institutions.

Community audits, where financial institutions conduct audits with other financial institutions that share the same cloud provider, would eliminate the redundancies and vulnerabilities created by duplicative monitoring. The requirements for a community audit would be the same as the individual audits that are presently conducted—focused on a cloud provider's controls for security and resiliency. Also, as is presently the case for audits conducted by individual institutions, these audits could be supported by an independent third-party audit firm with expertise in cloud technology. In addition to being more efficient, community audits would provide a forum for financial institutions to identify areas of common concern, and the results of an audit could be confidentially shared with regulators to increase overall assurance regarding cloud providers' security and control environments.

Of course, financial institutions will face practical challenges as to how such community audits would be conducted. Financial institutions would have to reach private agreements as to how the audit is funded and governed. They would also have to determine which other financial institutions would be included in a community audit, as financial institutions of varying size and sophistication will likely utilize the cloud differently and therefore have different security and resilience concerns. However, spreading costs of such an audit could establish a more level playing field between financial institutions by lowering the audit costs of individual financial institutions.

Collaborative bodies for addressing other kinds of technology-related risk could serve as a model for coordination between financial institutions. The Financial Services Information Sharing and Analysis Center (FS-ISAC), for example, is a nonprofit entity whose members include banks, credit unions, insurance companies, investment companies and financial services regulators. It was established in the late 1990s to collect and provide financial institutions with information on potential vulnerabilities as well as timely, accurate and actionable

warning of physical, operational and cyber-threats to the national financial services infrastructure. The FS-ISAC is run by its members, so its activities are tailored to the specific needs of the financial industry.[131]

Several financial supervisors, including the EBA and Australia's prudential regulator, have already acknowledged the value of the community audit approach.[132] Other regulators can facilitate cloud adoption by encouraging financial institutions to overcome collective action costs by issuing regulatory guidance that recognizes the ability—and utility—of financial institutions discharging their obligations to audit their cloud providers through controls audits performed as part of a community audit with other financial institutions.

Cross-border regulatory coordination

As noted earlier, another barrier to widespread cloud adoption by financial institutions is the cross-border nature of cloud services—specifically, the array of regulatory regimes to which cloud service providers and financial institutions are subject. Individual financial institutions and cloud providers are not well-positioned to manage issues arising from being subject to multiple, potentially disparate regimes governing data security and privacy. In addition, those overlapping regimes create a complex web of oversight that might fail to meet intended policy or supervisory goals. Accordingly, issues associated with the unique multi-jurisdictional nature of cloud services ought to be resolved in the first instance by direct cooperation between regulators.

To ensure consistency and predictability for market participants, regulators should seek consensus around shared substantive principles for regulating cloud use by financial institutions. However, it is also important for those substantive principles to be flexible enough that they are adaptable for use for a wide variety of cloud users and in different markets. In particular, they should be adaptable for jurisdictions with different levels of technological and financial maturity. To that end, instead of consensus on specific technical requirements or technological standards for security and resiliency, regulators should focus on developing risk-based principles for the use of cloud services by financial institutions.

Additionally, to the extent possible, these principles should encourage parity between foreign and local cloud service providers by facilitating the market access of foreign providers. Out-of-jurisdiction infrastructure is critical to the resiliency advantage offered by the cloud: the use of out-of-jurisdiction infrastructure makes it possible for financial institutions to distribute copies of applications or data to multiple locations (making them more difficult

---

[131] See generally Financial Services Information Sharing & Analysis Center, *Operating Rules*, FS-ISAC (June 2016), available at https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_June2016.pdf.

[132] See EBA, *Guidelines on outsourcing*, Section 13.3, par. 90 (cited in note 50). Australia's prudential regulator has also proposed a collaborative risk assurance model for cloud computing that would be "designed to meet the needs of the various customers". APRA, *Outsourcing Involving Cloud Computing Services* at 23 (cited in note 59).

to target) and route incoming application traffic across geographic regions (making cloud services more resilient to local failure).

Risk-based dialogue on industry-level risks

As financial institutions begin to migrate some of their core functions to the cloud, several regulators have identified cloud providers as potential sources of industry-level risk—for example, if a dominant provider relied upon by many financial institutions were to fail. There is currently minimal evidence of industry-level risk, as financial institutions still mostly rely on in-house technology infrastructure, especially for their core operations.[133] However, as the Financial Stability Board (FSB) explained in its recent report on market structure in financial services, "[i]f high reliance were to emerge, along with a high degree of concentration among service providers, then an operational failure, cyber incident, or insolvency could disrupt the activities of multiple financial institutions."[134]

Regulators should continue to assess and monitor potential industry-level risks arising from widespread cloud use, focusing on identifiable risk channels—specifically, those, if any, that are unique to the cloud in comparison to traditional technology infrastructure. In addition, they should take account of measures that cloud providers already take to mitigate the possibility of any single point of failure in their own infrastructure. These measures include compartmentalizing their infrastructure and services, including by isolating data centers from each other using redundant networking, connectivity and power. Major cloud providers also build in geographic diversity by providing even greater isolation from one region to another, such that even major physical catastrophes can be weathered. Ongoing assessment of industry-level risks must also weigh potential industry-wide risks against the benefits of cloud adoption, especially those related to increased security and resiliency.

A risk-based dialogue on industry-level risks should lead to greater understanding of the implications of more widespread cloud use by financial institutions. Given that cloud providers serve customers in a variety of different sectors, regulators also can benefit from enhanced collaboration with others outside the financial services sector, such as national security authorities and standards organizations, that interact with cloud providers on an ongoing basis and face many of the same concerns. Financial regulators may well conclude that the use of cloud computing by financial institutions does *not* pose novel risks to the financial sector—with the result that regulators and financial institutions alike should be more comfortable with migration to the cloud.

---

[133] See FSB, *FinTech and market structure in financial services* at 2 (cited in note 45) ("[R]eliance by financial institutions on third-party data service providers … for core operations is currently estimated to be low.").
[134] See id.

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