The Financial Services Sector's Adoption of Cloud Services

U.S. Department of the Treasury

Table of Contents

Executive Summary

The U.S Department of the Treasury (Treasury) and its partners in the Financial and Banking Information Infrastructure Committee (FBIIC) recognize the importance of assessing how trends in technology use could affect the operational resilience of the U.S. financial services sector. This report shares Treasury's findings on the current state of cloud adoption in the sector, including potential benefits and challenges associated with increased adoption. This report does not impose any new requirements or standards applicable to regulated financial institutions and is not intended to endorse or discourage the use of any specific provider or cloud services more generally.

Financial institutions of all sizes increasingly view services provided by cloud service providers[1] (CSPs) as an important component of their technology program, and cloud adoption could represent a significant change to financial institutions' internal operations and delivery of services to clients and customers.

Treasury found that the adoption of public cloud services[2] has increased rapidly over the last decade but that models of adoption continue to vary across the financial sector. Financial institutions have a wide range of use cases for cloud services, including supporting remote work environments and advancing innovation (for example, by harnessing cloud-native capabilities like artificial intelligence). Many financial institutions cited reduced costs, ability to rapidly deploy new information technology (IT) assets, shorter time to develop new products and services, and enhanced capabilities for security and resilience as motivating increased cloud adoption.[3] The COVID-19 pandemic has also accelerated cloud use given accelerated customer demand for innovative offerings through digital channels and financial institution demand to accommodate remote work. Treasury expects cloud adoption will continue to increase.

Cloud adoption can take a range of forms. Many larger financial institutions plan to adopt a "hybrid" model involving the strategic use of both public and private cloud services and their own data centers. Some financial institutions have significantly reduced their data center footprint by hosting applications and data in a public cloud environment. Smaller and mid-sized institutions are also adopting public cloud services, with some operating their IT infrastructure entirely in the cloud. Some cloud adoption is the result of acquiring cloud-native businesses. Other adoption is indirect and results from an institution's relationships with third-party providers, which have gravitated away from offering on-premises solutions in favor of cloud-based ones.

1. For the purposes of this report, a Cloud Service Provider (CSP) is an organization that provides cloud computing services to organizations other than itself.
2. This report is focused on how financial institutions use cloud services provisioned for open use by the general public, though observations in the report may be relevant to private cloud services as well.
3. Such motivations are not unique to financial services. As detailed in Annex A, Treasury has developed a strategy to harness the potential efficiency, elasticity, scalability, and security capabilities associated with cloud services.

In assessing the current state of cloud adoption in the financial sector, Treasury identified six thematic challenges described below and expanded on in Section 6 of this report. These challenges, if unaddressed, may detract from the potential benefits associated with cloud services. Some of challenges may also be more acute for small and medium-sized financial institutions.

Insufficient Transparency to Support Due Diligence and Monitoring by Financial Institutions: Risk management of any third-party service requires the financial institution to understand the risks associated with that service. Treasury encountered a range of views on whether the information being shared by CSPs was sufficient to understand risks. Early adopters and financial institutions that brought significant scale to their use of cloud services were often the most satisfied with the information they received. However, Treasury met with several financial institutions that wanted additional information to improve their understanding of the risks associated with cloud services. Areas of interest included: (i) internal software dependencies within the public cloud environment; (ii) subcontractor and other supply chain risks; (iii) CSP protection against pervasive cyber vulnerabilities; (iv) results of testing resilience and security capabilities; and (v) information regarding operational incidents, including real-time updates and after-action reports.

Treasury understands that CSPs limit physical access and refrain from sharing sensitive information to reduce risk to their infrastructure. CSPs have noted that intensive in-person audits are challenging to accommodate at scale while maintaining the security of the multi-tenant environment. Similarly, financial institutions, particularly small and medium-sized financial institutions, noted that third-party risk management was becoming increasingly complex and resource-intensive. Treasury is aware that the industry is considering and implementing a range of alternative approaches to one-to-one audits, like pooled audits, certifications, or real-time updates to customers. Treasury encourages efforts that could yield efficiency gains for both CSPs and financial institutions without compromising outcomes.

Gaps in Human Capital and Tools to Securely Deploy Cloud Services: Public cloud services are deployed using a "shared responsibility model," which requires both CSPs and financial institutions to take actions to secure and monitor the cloud environment (though the division of responsibility will vary depending on the service being offered). Many security incidents are caused by user misconfiguration of cloud services. Treasury identified two issues that can increase the frequency of user misconfiguration. These issues are particularly acute for small and medium-sized financial institutions.

First, there is a shortage of appropriate staff expertise for cloud services. General IT and cybersecurity skills may not fully translate to the cloud environment without additional training. Skills associated with deploying and securing applications on one CSP do not necessarily translate to other CSPs. The scarcity of relevant experts may become increasingly pressing if cloud adoption increases.

Second, certain cloud service offerings can be highly complex for financial institutions to implement, design, and manage. The tools offered in cloud environments may not always be user-friendly. Financial institutions expressed a desire for further guidelines on baseline configurations, from the CSPs or public sector, and continued evolution in cloud-related tools, such as those for security configuration and monitoring. Some firms reported occasional differences in how service features were documented in CSP-provided client materials and how the features actually functioned.

Exposure to Potential Operational Incidents, Including Those Originating at a CSP: While cloud services can offer potential benefits to resilience and security that could result in reduced operational risk overall, these services are still vulnerable to operational incidents, like any technology utilized by financial institutions. Financial institutions are still developing configurations to best protect against an operational incident that could affect more than one geographic region of a CSP. However, these configurations may still be vulnerable to an incident affecting multiple geographic regions or services integral to the cloud environment, such as identity and access management.

Financial institutions can configure cloud services with different levels of resilience to operational incidents, but options offered by CSPs will vary depending on the service. Financial institutions will generally configure cloud services for a higher level of resilience when those services support critical applications for their core businesses. Options for resilience configuration generally include (i) relying on a single CSP (through single or multiple regions), (ii) using separate CSPs for different applications, or (iii) combining public and private cloud with on-premises infrastructure. There are potential benefits and challenges with each of these approaches. However, these options add additional costs.

Greater substitutability between CSPs might partially address this challenge, but many practitioners noted that running the same application on two or more CSPs simultaneously can be impractical. No financial institution reported the capability to do so for more complex use cases, such as running core operations on multiple public clouds. Running an application across multiple CSPs at the same time may also be less desirable, given the costs, staffing, and complexity involved in doing so, particularly given the complexity associated with identifying and managing risk across multiple cloud environments.

Potential Impact of Market Concentration in Cloud Service Offerings on the Sector's Resilience: The current cloud services market is concentrated around a small number of service providers. Financial institutions can also rely indirectly on other third-party providers that may also use the same small number of CSPs. The scale these CSP firms offer can have potential benefits, like economies of scale to support investments in cybersecurity and resilience. And services run on the cloud environment can be patched quickly to protect against zero-day exploits. Scale may also help facilitate more interoperability between financial institutions and their vendors.

On the other hand, concentration could expose many financial services clients to the same set of physical or cyber risks (e.g., from a region-wide outage), and addressing such risks may necessitate action on the part of each financial services client. But the impact from an operational incident will depend on how individual financial institutions use and manage the cloud service and how critical that service is to the financial institutions' core operations. The key issue for policymakers and financial authorities is in understanding the potential aggregate impacts on financial institutions' functions and the services that financial institutions provide to consumers and businesses.

Data limitations prevent Treasury and the FBIIC from fully assessing the significance of the concentration in cloud services across the sector. For example, there is currently no common approach within the financial sector to measure critical uses of cloud services by financial institutions, making it difficult for financial regulators to aggregate data.

U.S. financial regulators assess risks based on information provided by financial institutions they supervise. Regulators can also evaluate how supervised financial institutions manage such risks. However, due to the different legal authorities for each agency, no single agency can see across the many use cases and the network of dependencies on cloud services within the financial sector. FBIIC-member agencies have channels for formal and informal cooperation to help develop a more comprehensive view, though Treasury assesses that these channels can be enhanced. Treasury will prioritize its focus on studying the concentration of cloud services most important to the functions of the financial sector. Treasury also believes there are opportunities to enhance public-private coordination given the broader trends in cloud adoption. For example, many organizations have not yet incorporated CSPs into sector-wide protocols for incident response.

Dynamics in Contract Negotiations Given Market Concentration: Discussions revealed that financial sector firms of all sizes consider negotiating contracts with CSPs to be challenging. Smaller financial institutions noted their lack of bargaining power. Early adopters of cloud services noted that it was particularly difficult to negotiate for audit rights and avoid termination by the CSP without notice. Some financial institutions noted it was important to address the disposition of encryption keys. Larger financial institutions have been able to negotiate some custom provisions but on a limited basis. Treasury will continue to assess this issue, as unbalanced contractual terms could limit individual financial institutions' ability to measure and mitigate risks from cloud services, which could result in unwarranted risk across the sector.

International Landscape and Regulatory Fragmentation: Increased foreign regulatory scrutiny of cloud services and CSPs could pose benefits and risks to the resilience, security, and capabilities of cloud services used by U.S. financial institutions. International regulatory concern over cloud services also has the potential to prevent globally active U.S. financial institutions from deploying cloud services across their overall enterprise, including their foreign operations.

Next Steps

Treasury believes that the six aforementioned challenges should continue to be monitored and addressed to promote the continued resilience of the financial sector. To promote coordination and collaboration among U.S. financial regulators on these challenges, Treasury will establish a Cloud Services Steering Group. Treasury will also facilitate further engagement between the financial sector and CSPs. Treasury's next steps will be guided by its Strategic Vision for Supporting the Resilience of the Financial Sector's Use of Cloud Services.

Treasury's work (further described in Section 7) will include the following:

- Promoting closer domestic cooperation among U.S. regulators on cloud services;
- Conducting tabletop exercises with industry;
- Reviewing sector-wide incident protocols in light of growing reliance on cloud services;
- Considering ways to appropriately measure cloud service dependencies across the sector and assessing systemic concentration and related risks on a sector-wide basis; and
- Identifying ways to foster effective risk management practices in the financial services industry.

Recognizing that many U.S.-based cloud providers are also active globally, Treasury, along with FBIIC-member agencies, will continue to support the development of relevant standards and international policies at the G7, the Financial Stability Board, and the international financial standard-setting bodies, and explore ways to increase international collaboration and coordination on financial regulatory issues arising from cloud services.

Treasury's Strategic Vision for Supporting the Resiliency of the Financial Sector's Use of Cloud Services

Treasury has developed long-term objectives to promote the financial sector's operational resilience with the use of cloud services. This strategic vision will guide Treasury's engagement in the coming months and years with the private sector, as well as with domestic and foreign counterparts.

PREAMBLE

- Treasury, U.S. financial regulators, regulated financial institutions, and CSPs have similar objectives for the operational resilience of the financial sector. In the face of an increasingly complex threat environment, including from hostile actors, effective outcomes for sector level resilience require trust, cooperation, and collaboration among these stakeholders.
- Treasury, as Sector Risk Management Agency for the financial sector, will periodically assess risks and challenges that could affect the financial sector arising from widely used technology services, like cloud services.
- In doing so, Treasury will seek assistance from other stakeholders, including:
- U.S. financial regulators, which (to the extent consistent with their mandate) are responsible for assessing risks to individual financial institutions.
- CSPs, which are responsible for providing services in a manner consistent with agreed-upon service levels, including with regard to security and reliability.
- Financial institutions, which are ultimately responsible for their own operational resilience and for taking steps to identify, measure, monitor, and manage the risks from services that they select, consistent with their regulatory requirements.
- Other government agencies, like the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), that play a

role in promoting effective practices and leading U.S. government engagement on cybersecurity risks.

- Treasury will work with these stakeholders to address issues arising from cloud services use that could impact the operational resilience of the sector, including with respect to financial stability.

RISK ASSESSMENT AND MITIGATION:

- Effective practices for financial institutions include taking a risk-based approach to their chosen cloud service offerings.
- The risk and benefits of these services depend on how financial institutions use, design, and implement services. Effective cloud adoption by financial institutions requires specialized expertise. Different services may have different levels of criticality or importance from one financial institution to another.
- Financial institutions can address cloud-related risks in a variety of ways, including by designing for resilience and communicating their expectations for operational resilience and security to CSPs.
- Transparency from cloud providers, including over potential risks and vulnerabilities, is critical to enable financial institutions to select and configure service offerings consistent with their risk appetite.
- Contractual commitments between financial institutions and CSPs should support the risk management needs and responsibilities of financial institutions.

SECTOR-WIDE CONCENTRATION:

- Policymakers and financial regulators should continue to study concentration in cloud services, assessing the potential for system-wide impacts.
- To assess the implications of sector-wide concentrations related to financial institutions' operational resilience, financial authorities must continue efforts to understand the criticality of a cloud service to a financial institution's business functions and operations.
- Treasury will prioritize its focus on the concentration of cloud services most important to the functions of the financial sector.
- If Treasury assesses that cloud services critical to the functioning of the financial sector do not have appropriate resilience and security, Treasury will take actions as appropriate and consistent with its authorities in consultation with appropriate government agencies.
- Communication and engagement by government authorities, including from Treasury and the financial regulators, can inform how the private sector manages risks and help foster public-private collaboration. Treasury and FBIIC members should continue

maturing strategies for incident response and coordination associated with cloud services (involving other government agencies where needed).

- Understanding potential system-wide risks associated with cloud services requires appropriate coordination and information sharing among the U.S. financial regulators and with Treasury.[4]
- Regulatory fragmentation or gaps in coordination among financial authorities and jurisdictions has the potential to negatively impact the resilience or security of cloud services, and, ultimately the users of these services, such as U.S. financial institutions and the U.S. government.
- Treasury will continue supporting international efforts related to cloud services, including work at standard-setting bodies to promote alignment around clear and effective approaches to regulate and supervise financial institutions' use of cloud services.
- Treasury believes that there are opportunities for U.S. and foreign jurisdictions to collaborate in addressing potential risks of cloud services to the global financial system while limiting unintended negative consequences.

4. There are a number of existing models for this type of collaboration, such as formal or informal channels among U.S. regulators or through the FBIIC.

ACRONYMS PAGE

ABA	American Bankers Association
ACSSS	American Council of State Savings Supervisors
AI/ML	Artificial Intelligence/Machine Learning
API	Application programming interface
AWS	Amazon Web Services
BCBS	Basel Committee on Banking Supervision
BSCA	Bank Service Company Act
CEG	G7 Cyber Expert Group
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Agency
COBIT	Control Objectives for Information and Related Technologies
CSBS	Conference of State Bank Supervisors
CSP	Cloud Service Provider
DCO	Derivatives Clearing Organization
DFMU	Designated Financial Market Utility
DORA	Digital Operational Resilience Act
ESA	European Supervisory Authority
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
FMU	Financial Market Utility
FRB	Federal Reserve Board
FSB	Financial Stability Board
FSSCC	Financial Services Sector Coordinating Council
GCP	Google Cloud Platform
GLBA	Gramm-Leach-Bliley Act
IaaS	Infrastructure-as-a-Service
IAIS	International Association of Insurance Supervisors

IAM	Identity and Access Management
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
IDC	International Data Corporation
JAB	Joint Authorization Board
NAIC	National Association of Insurance Commissioners
NASAA	North American Securities Administrators Association
NASCUS	National Association of State Credit Union Supervisors
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
NPI	Nonpublic Personal Information
OCC	Office of the Comptroller of the Currency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
OMB	Office of Management and Budget
PaaS	Platform-as-a-Service
PAM	Privileged Access Management
PFMI	Principles for Financial Market Infrastructure
Reg SCI	Regulation for Systems Compliance and Integrity
SaaS	Software-as-a-Service
SEC	Securities and Exchange Commission
SLA	Service-Level Agreement
SOC	Service Organization Controls
SRMA	Sector Risk Management Agency
SSB	Standard-Setting Body

Introduction

2.1 Background on FBIIC and the purpose of this report

FBIIC is a Treasury-chaired committee composed of 18 federal and state financial regulatory organizations.[5] The FBIIC is charged by the President's Working Group on Financial Markets with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial services sector, and enhancing the resiliency of the financial sector overall. As part of the FBIIC's ongoing review of cybersecurity trends and issues in the financial sector, Treasury leadership commissioned this report to explore how the use of cloud services may affect the sector's operational resilience.

In consultation with a working group of ten FBIIC-member organizations,[6] Treasury developed this report through:

- Research on how the financial services sector uses cloud services, the legal and regulatory authorities available to U.S. financial regulators, regulatory activity and observations, and FBIIC-member priorities and experiences; and,
- Consultation with market participants and other stakeholders (described in Annex B). Stakeholders included: financial sector trade associations, research-focused think tanks, depository institutions, insurance companies, financial market utilities (FMUs), CSPs, financial sector technology service providers, and payment networks.

2.2 HOW THE REPORT IS ORGANIZED

The report is organized around five main topics, beginning with Section 3, *Cloud Use in Financial Services*. This first section summarizes information gained from federal and state financial regulators' observations of cloud use among their regulated entities, as well as from stakeholder feedback, including sector motivations for cloud adoption. The next section, *Domestic and International Regulatory Framework,* contains a discussion of the U.S. regulatory framework for financial services firms' use of cloud services, as well as a discussion of international approaches. The third section, *Financial Institution Practices When Adopting Cloud Services*, describes various approaches to cloud migration and the steps financial sector participants typically consider when migrating to cloud. The fourth section, *Challenges with Adoption,* summarizes Treasury's observations regarding key

5. The FBIIC member organizations are: the U.S. Department of the Treasury (Chair), American Council of State Savings Supervisors (ACSSS), Consumer Financial Protection Bureau (CFPB), Commodity Futures Trading Commission (CFTC), Conference of State Bank Supervisors (CSBS), Farm Credit Administration (FCA), Federal Deposit Insurance Corporation (FDIC), Federal Housing Finance Agency (FHFA), Federal Reserve Banks of Chicago and New York, The Board of Governors of the Federal Reserve System (FRB), National Association of Insurance Commissioners (NAIC), National Association of State Credit Union Supervisors (NASCUS), National Credit Union Administration (NCUA), North American Securities Administrators Association (NASAA), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), and the Securities Investor Protection Corporation (SIPC).
6. Experts from the CFPB, CFTC, CSBS, FDIC, FHFA, FRB, NASAA, OCC, and SEC assisted Treasury with developing this report.

challenges associated with increased cloud adoption experienced by financial institutions, CSPs, and financial regulators. The final section, *Areas for Further Consideration and Next Steps,* outlines Treasury's short-term actions and long-term objectives regarding the financial sector's adoption of cloud services.

2.3 BACKGROUND ON CLOUD SERVICES

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or CSP interaction.[7] Although computer scientists had described several of the essential characteristics of cloud computing by the mid-twentieth century, the development of cloud services has accelerated in the last twenty years due to advancements in virtualization and other technologies, networking, connectivity, and reduction in costs of hardware and other components.[8]

An organization may provide cloud computing resources via several forms: (i) **public cloud**, which is available to the general public on existing infrastructure owned by a cloud provider, (ii) **private cloud**, which is available for exclusive use by a single organization on or off of their premises, (iii) **community cloud**, which is available for use by a specific community of users, or (iv) **hybrid cloud**, which combines elements of the preceding three deployment models.[9] Stakeholders also use the term hybrid cloud to describe the preceding cloud models in combination with on-premises architecture. The figure on the following page illustrates the essential characteristics, service models, and deployment models of cloud services.

Cloud computing is a substantial proportion of the worldwide IT market, consisting of hardware, software, data centers, networking, and numerous other products and services. According to Gartner, a technological research and consulting firm, public cloud services spending grew from $220 billion in 2016[10] to $411 billion in 2021, and it is estimated to reach nearly $600 billion in 2023.[11] Surveys of Chief Information Officers (CIOs) confirm that a substantial and growing proportion of IT spending at enterprise organizations is dedicated to public cloud services. One recent survey indicates 72 percent of CIO respondents expect their organization to increase their public cloud spending over the next year, while 49 percent expect to increase their private cloud and on-premises spending.[12]

7. NIST, Special Publication 800-145, The NIST Definition of Cloud Computing (Sep. 2011), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.
8. Garfinkel, Simson, *The Cloud Imperative*, MIT Technology Review (Oct. 2011), https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative.
9. NIST SP 800-145
10. Gartner, *Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach $260 Billion in 2017* (Oct. 2017).
11. Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023 (Apr. 2022), https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022.
12. Barclays Equity Research, *Cloud Wars; Vendor Positioning and Private vs. Public*, by Long, Tim; Wang, George; Shreves, Alyssa (May 2022).

Figure 1: NIST Definition of Cloud

Essential characteristics	On-Demand Self-Service	User can unilaterally provision server time, network storage, etc. as needed without involving service provider.
	Broad Network Access	Capabilities are available over the network and accessed through common mechanisms (e.g. a Web browser) and devices.
	Resource Pooling	Physical and virtual resources are shared across a large pool of users, allowing for dynamic assignment according to users' demands.
	Rapid Elasticity	Computing capabilities can be scaled rapidly up or down according to users' demands, such that any given user's demand is met without interruption.
	Measured Service	Users access capabilities as a service and pay only for resources used.
Service models	Software-as-a-Service (SaaS)	End-user applications provided as a service only. User cannot manage or control any underlying cloud infrastructure.*
	Platform-as-a-Service (PaaS)	Application platforms or middleware provided as a service on which users can build and deploy custom applications using programming languages, libraries and other tools supported by service provider.
	Infrastructure-as-a-Service (IaaS)	Broad and scalable computing capabilities provided as a service, including processing, storage, networks, and operating systems, enabling more control over deployed applications.
Deployment models	Public Cloud	The cloud infrastructure is available for open use by the general public. It generally is owned by and exists on the premises of the cloud service provider.
	Private Cloud	The cloud infrastructure is available for exclusive use by a single organization. It may exist on or off premises and may be owned by the organization, a third party, or both.
	Community Cloud	The cloud infrastructure is available for use only by a specific community of users that have shared needs or concerns. It may be owned by one or more of the community users, by a third party, or some combination.
	Hybrid Cloud	The cloud exists as a configuration of two or more distinct cloud infrastructures (public, private, or community) that enables data and application portability among the separate infrastructures.

* Cloud infrastructure includes network, servers, data, middleware, operating systems, storage, etc.

Source: National Institute of Standards and Technology.

This report will use the three main service models described in the NIST definition of cloud computing to characterize cloud adoption. In 2021, according to International Data Corporation (IDC),[13] the SaaS applications segment was the largest of all cloud market segments, measuring $178 billion, growing 24 percent over the prior year. IDC estimates that Microsoft[14] led the SaaS market (11 percent) followed by Salesforce (10 percent), SAP (5 percent) Oracle (4 percent), and Google Cloud Platform (GCP) (3 percent).

13. International Data Corporation, *Worldwide Semiannual Public Cloud Services Tracker H2-2021.*
14. Cloud services offered by each of these market participants may be conducted through multiple business lines and across legal entities within each organization. For the purposes of this report, services provided by "AWS" and "GCP" generally refers to all cloud services provided across the corporate families of each. References to "Microsoft Azure" refer primarily to IaaS, PaaS, and some SaaS services provided by Microsoft (but not Microsoft Office 365 and Exchange Online).

The IaaS segment is the second largest segment, with projected spending of $115 billion.[15] It is also expected to be the fastest growing cloud segment, with projected growth in 2023 at nearly 30 percent.[16] Analysts have identified three dominant CSPs, with some estimates placing the top three CSPs with over 66 percent of the total worldwide market share in IaaS. According to one measurement of public IaaS cloud services in 2021, AWS's revenue comprised nearly 39 percent of the worldwide IaaS segment, followed by Microsoft Azure at 21 percent, and GCP at 7 percent. Two foreign providers, Alibaba and Huawei, also compete with 10 percent and 5 percent of worldwide market share, respectively.[17]

The PaaS segment is the third-largest public cloud services segment worldwide, with projected spending in 2022 of $111 billion.[18] Views on market leadership in the global PaaS segment are mixed; for example, one recent CIO survey identifies Microsoft Azure as the market leader, followed by Amazon Web Services (AWS) and GCP,[19] while another identifies Microsoft Azure as leading, followed by Salesforce, GCP, and AWS.[20] VMWare, IBM, and Oracle are other providers with offerings in both the IaaS and PaaS segments.

2.4 U.S. GOVERNMENT APPROACH TO CLOUD COMPUTING

Elements of this report are informed not just by Treasury's engagement with interested stakeholders but also by its experience in modernizing its own IT infrastructure. The use of cloud computing has been an important element of the U.S. Government's longstanding effort to modernize its IT infrastructure and improve cybersecurity across U.S. agencies. In May 2021, President Biden issued Executive Order 14028 (E.O. 14028), Improving the Nation's Cybersecurity, articulating a vision of "Zero Trust Architecture" for Federal Government networks. NIST defines zero trust as "[a] collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."[21] Zero trust is a security model that assumes threats exist inside and outside of network boundaries, continuously scans for anomalous or malicious activity, and limits access to only what is necessary to perform required jobs and protect data in real-time.[22] E.O.14028 also stipulates that the "Federal Government must … accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)." In accordance with E.O. 14028, Office of Management and Budget (OMB) published a Federal zero trust strategy that calls upon U.S. agencies to define and implement cloud-based infrastructure to support their zero

15. Gartner, *Gartner Forecasts Worldwide Public Cloud End-User Spending.*
16. Ibid.
17. Gartner, *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 41.4% in 2021* (Jun. 2022), https://www.gartner.com/en/newsroom/press-releases/2022-06-02-gartner-says-worldwide-iaas-public-cloud-services-market-grew-41-percent-in-2021
18. Gartner, *Gartner Forecasts Worldwide Public Cloud End-User Spending.*
19. Morgan Stanley Research, *1Q22 CIO Survey: A Surprisingly Durable View on Growth.*
20. Goldman Sachs Equity Research, *IT Spending Survey: 2022 Outlook Solid*.
21. NIST, Zero Trust Architecture, by Rose, Scott, et al (Aug. 2020), https://csrc.nist.gov/publications/detail/sp/800-207/final
22. "Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity." 86 Fed Reg. 26633.

trust models,[23] and CISA published technical reference architecture to provide agencies guidance on such implementation.[24]

Zero trust-related initiatives over the last eighteen months represent an acceleration of efforts to use cloud services to modernize U.S. agencies' technology infrastructure, which began with the OMB's "cloud-first" Federal Cloud Computing Strategy[25] and development of the Federal Risk and Authorization Management Program (FedRAMP).[26] FedRAMP promotes secure cloud adoption across the Federal Government by creating standardized security requirements for the authorization and ongoing cybersecurity of certain cloud services. This approach enables individual agencies or the Joint Authorization Board (JAB) to work directly with cloud providers to review the security of individual services and conduct remediation as required. Federal agencies can review and reuse cloud service offering packages once they are designated as "Authorized" in the FedRAMP marketplace, enabling multiple agencies to leverage assessments conducted during the initial authorization process.[27] After authorization, cloud providers must continuously monitor the security state of their cloud service offerings, conduct remediation as required, and comply with incident reporting requirements.[28] Treasury's own experience with cloud services is described in Annex A.

23. OMB, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, (Jan. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
24. CISA, *Cloud Security Technical Reference Architecture* (June 2022), https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf.
25. OMB, *Federal Cloud Computing Strategy* (Feb. 2011), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.
26. OMB, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 2011), https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf.
27. See, for example, https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook. pdf. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Marketplace_Designations_for_Cloud_Service_Providers.pdf.
28. GSA, *FedRAMP Incident Communications Procedures* (Apr. 2021), https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

Cloud Use in Financial Services

3.1 MOTIVATIONS SUPPORTING CLOUD ADOPTION AND TYPES OF CLOUD SERVICES

Over the past decade, financial institutions[29] have been increasing their use of cloud services, ranging from video conferencing and collaboration software to banking and trading platforms that support internal operations and business line functions. This trend exists across both small and large financial institutions. Some smaller financial institutions conveyed that they felt cloud adoption was imperative for their continued viability for some of the reasons indicated below.

Primary drivers for the financial sector's migration to cloud services include the following:

- Faster development and scaling of new applications and services using cloud infrastructure and tools, particularly for artificial intelligence and consumer-facing applications, such as mobile banking and trading;
- The ability to meet competitive challenges and customer demands for digital financial products with robust features and data, supported by cloud services to interface with a range of partner financial institutions and non-banks;
- The potential for increased resilience to physical and cyber incidents, with the use of multiple data centers or regions from the same CSP and broader use of encryption and zero trust models;
- Third-party providers migrating to cloud services and discontinuing existing on-premises product offerings for client financial institutions;
- The potential for lower costs when compared to a legacy IT environment; and,
- The need for a substantial expansion in IT infrastructure to support remote workers and customers' use of digital financial services, hastened by the COVID-19 pandemic.

The customizable nature of cloud services allows a financial services firm – consistent with its responsibilities – to select or design a cloud service that meets its business, security, risk tolerance, resilience, and operational needs. A "shared responsibility" model typically governs cloud services, which covers the responsibilities of the CSP (as the service provider) and the financial services firm (as the client), including those concerning security obligations. A CSP typically provides the various service options for the client and commits in the contract and other service documentation to maintain specific baseline security, performance, and resilience controls for the purchased cloud service. The contract will specify the responsibilities of either the vendor or client with respect to the evaluation and selection of the service architecture and the design and implementation of related security

29. The focus of this report is on how cloud services are being adopted by financial institutions subject to supervision and regulation by FBIIC members. Section 3.1 to section 3.5 of this report discusses how cloud services are being used across the financial services sector, and section 3.6 to 3.8 provides details on specific components of the financial services sector. See Section 4.1 for additional information on the specific institutions and authorities within the purview of individual agencies.

and resilience controls. This responsibility will vary between the three cloud deployment models: IaaS, PaaS, and SaaS. Notwithstanding these contractual terms, a financial services firm remains ultimately responsible for the operational resilience of its business, including functions that rely on the use of cloud services.

3.2 POTENTIAL BENEFITS OF CLOUD COMPUTING TO OPERATIONAL RESILIENCE

Industry practitioners and other technical experts generally believe that when configured correctly, public cloud services can provide an environment that is resilient and secure. But the resilience and security of any particular cloud service can and will vary depending on the vendor and service, as well as how each service is configured, provisioned, and managed. Not all of these features may be available in all circumstances.

REDUNDANCY

Cloud services offer physical redundancy beyond what most financial institutions could develop independently. Some CSPs structure cloud services to operate from multiple "availability zones," which are physically or logically isolated data centers that host cloud services.[30] The availability zones are usually grouped into regions (e.g., U.S. east coast vs. U.S. west coast), with the major cloud providers offering multiple regions across the globe. The architecture underpinning public cloud services may allow clients to maintain completely synchronized data sets at various data centers within an availability zone, resulting in little or no data loss if a client switches from primary deployment to redundant options. Each data center region is intended to be isolated to limit the probability of concurrent disruption. But because cloud services are usually delivered through the internet, CSPs and financial institutions may rely on data communications service providers to provide uninterrupted data communications. Though some on-premises configurations used by financial institutions may be similarly reliant on data communication service providers as well.[31]

SCALABILITY AND SPEED TO DEPLOY ASSETS

The ability to rapidly procure and commit new resources may be the most attractive feature of cloud services to financial institutions. Cloud services are deployed over the internet and are also generally not subject to bandwidth limitations of traditional virtual private networks.

Intermittent workloads, like risk modeling or development environments on the public cloud, are common use cases for financial institutions that benefit from the scalability of the cloud environment. Being able to deploy limited-use resources quickly on an IaaS

30. Specific implementation of these concepts, e.g., physical vs. logical isolation, size and capacity of a region or availability zone can vary. See Amazon, Regions and Availability Zones, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/, Google, Regions and Zones, https://cloud.google.com/compute/docs/regions-zones Microsoft, What are Azure regions and availability zones?, https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview.
31. Cloud configurations may not always be reliant on data communication services providers, because some CSPs operate their own global networks to facilitate the movement of data within the cloud and some clients may have direct private connections to their CSPs.

environment can also offer a more flexible testing environment for financial institutions, which helps support the transition to a more secure software development pipeline based on continuous integration and deployment for financial institutions that develop or modify their software.

Experts note that the capability to scale resources could allow financial institutions to add three-, five-, or ten-x capacity to support existing workloads. Financial institutions conveyed that efforts to develop this capability for core processing activity were still at the theoretical stage. In their view, public cloud services appeared to be the most viable means to achieve this type of "burst capacity." Assuming that relevant workloads were fully deployed on the cloud environment, this type of capability could be valuable during a period of heightened market stress requiring more transactions to be processed.

SECURITY

From the perspective of the financial institutions interviewed for this report, the security capabilities for public cloud services generally match or exceed their on-premises capabilities. For example, a number of stakeholders mentioned that the built-in logging capabilities associated with many IaaS services are often superior to their on-premises capabilities for their own assets deployed on the cloud. Cloud services also enable financial institutions to encrypt data more readily at rest and in transit. Some CSPs also have processes to address lesser-known security risks, like vulnerabilities through individual components, by fully securing their hardware supply chain.

However, some financial institutions had challenges in making such determinations regarding the security capabilities provided by CSPs based on the current level of the information supplied by CSPs. For example, some financial institutions indicated they wanted to know more about CSPs' internal software dependencies, testing results, and other processes relevant to assessing how CSPs address risks to the cloud environment. It also can be challenging for financial institutions to manage the integration of cloud services with their on-premises IT infrastructure. As a result, there could be differences between theoretical security capabilities and actual results. These issues are further explored in Section 6.

3.3 SHARED RESPONSIBILITY

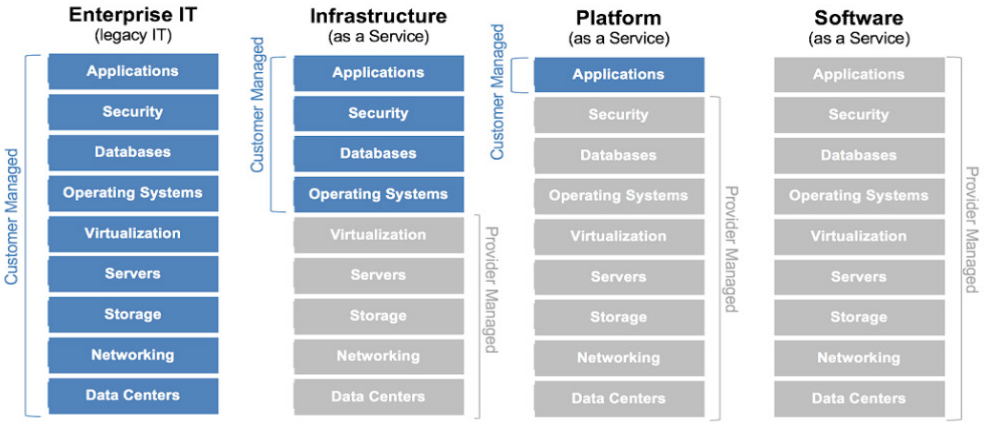
It is common practice for CSPs to assume specific technical, administrative, and physical security responsibilities for certain underlying aspects of the cloud service. For example, CSPs in the IaaS model are generally responsible for securing the IT hardware and the single or multi-tenant environment in which the hardware resides, while the financial institution is typically responsible for setting the security controls for the operating systems and applications placed in the IaaS environment. In a SaaS model, the CSP is customarily responsible for securing all aspects of the SaaS application and its operating

environment. At the same time, the financial institution is usually responsible for securing its access to the application. The level of the CSP's involvement and control over the security and other operational aspects of the cloud service generally increases along the continuum of IaaS to SaaS.

This approach to allocating management of service architecture and security and resilience controls for cloud services between the financial institution and the CSP is generally referred to as a "shared responsibility" approach, which makes it more practical to scale public cloud services across thousands of clients.[32] The contract between the CSP and the client typically cover their respective responsibilities in the event there is an operational or cyber incident (like expectations around initial notification). Notwithstanding the shared responsibility approach, financial institutions are ultimately responsible for managing the risks of a CSP relationship and for the security of all their information assets, including those deployed on the cloud. To fulfill this responsibility, financial institutions will generally conduct a risk-based evaluation of cloud service(s) and determine if security and resilience controls (whether under the nominal purview of the financial institution or the CSP) are commensurate with the security obligations and risk posture of the financial institution. Section 5 contains further discussion of financial institution practices, and Section 6 describes challenges and tensions arising from the shared responsibility model.

The graphic below shows one example of an allocation approach of operational and security management associated with CSP and its customer entities. The approach may vary for different CSPs, the cloud services they provide, and the customers they serve.

Figure 2: Security Responsibilities Between Clients and CSPs



Source: GSA, Cloud Information Center, https://cic.gsa.gov/basics/cloud-security

32 GSA, Cloud Information Center, https://cic.gsa.gov/basics/cloud-security.

3.4 TYPES OF CLOUD SERVICES USED BY FINANCIAL INSTITUTIONS

3.4.1 SOFTWARE AS A SERVICE (SAAS)

SaaS is currently the most widely adopted cloud service by financial institutions. For example, one survey estimated adoption in the banking industry around 91 percent.[33] Similar to traditional outsourcing, financial institution management does not directly manage, maintain, or control the underlying cloud infrastructure or individual application capabilities of the SaaS application. Rather, the SaaS provider manages the underlying software application and the cloud infrastructure on which the SaaS application resides. In addition to managing the overall risk of its relationship with the CSP, under the SaaS model, financial institutions typically retain operational responsibility for the data transmitted and stored in the SaaS application, user-specific application configuration settings, setting user access rights, and monitoring use. The CSP is responsible for any changes to and maintenance of the applications and infrastructure. Common SaaS applications include office productivity systems, compliance tools (such as anti-money laundering tools), order/portfolio management systems, and security monitoring tools. Financial institutions generally find SaaS applications to be the easiest cloud-based services to deploy and manage. For example, it is common practice among small and large institutions to use cloud-based versions of traditional software applications like email.

Many traditional third-party financial technology service providers are expanding their product lines to include cloud-based software versions of their core banking and trading software. A vast number of third-party service providers may provide their financial institution customers with applications that rely on CSP-provided SaaS.

3.4.2 PLATFORM AS A SERVICE (PAAS)

Financial institutions use PaaS to support software development and deploy security tools, often in conjunction with their use of IaaS. These applications reside on the provider's platforms and cloud infrastructure. PaaS models necessitate similar risk management as the SaaS model. However, a financial institution is additionally responsible for the appropriate provisioning and configuration of cloud platform resources and implementing and managing controls over the development, deployment, and administration of applications residing on the provider's cloud platforms. The CSP is responsible for the underlying infrastructure and platforms (including network, servers, operating systems, or storage). Financial institutions' current use of PaaS services is significant but substantially smaller than their use of SaaS cloud services. According to a survey conducted in 2021 by the American Bankers Association, 43 percent of the surveyed financial institutions with cloud deployments used PaaS cloud applications. This number was projected to increase to 64 percent in the next two years.[34]

33 American Bankers Association, *Cloud Computing in the U.S. Banking Industry* (Jun. 2021).
34 Ibid.

3.4.3 INFRASTRUCTURE AS A SERVICE (IAAS)

Financial institutions commonly use IaaS to support in-house developed or acquired core processing platforms, as well as to support data storage, business recovery, and to increase the efficiency, agility, and scalability of their IT infrastructure. Some financial institutions employ a hybrid model with an on-premises data center supported by data storage and computing facilities in a public cloud that can be accessed to support large scale processing and storage demands or backup functions as needed.

Like PaaS, IaaS arrangements usually make the financial institution responsible for appropriately provisioning and configuring cloud platform resources, and implementing and managing controls over operations, applications, and data. Additionally, the IaaS model typically places responsibility on financial institutions for networks, servers, operating systems, and storage. Financial institution management may need to configure the institution's enterprise systems to work with the CSP's resilience and recovery process. The CSP is responsible for controls related to managing the physical data center. For example, the CSP updates and maintains the hardware, network infrastructure, environmental controls (e.g., heating, cooling, and fire and flood protection), power, physical security, data communications connections, and the "lynchpin" services that underpin and are necessary for the provision of many cloud services (e.g., domain name systems, identity access management, virtualization firmware or hardware).

A 2021 survey by American Bankers Association (ABA) revealed that IaaS is the least commonly used cloud service by banks, with 29 percent of the surveyed using IaaS applications in cloud. Respondents, however, expected this to increase to 52 percent in the next two years.[35]

3.4 PRIVATE VS. PUBLIC CLOUD

Public cloud is a cloud computing model in which services and infrastructure are managed and maintained by a third-party provider and shared with multiple users remotely through the public internet. Data centers utilize a multi-tenant system in which users share access to services and host data on the same servers. Public cloud eliminates the need for organizations to host and maintain services in internal data centers, reducing the cost of on-site systems and associated operational challenges.

In a private cloud, computing services are provisioned for exclusive use by a single organization.[36] Private clouds can be hosted either on-premises or through a CSP that maintains private data centers. The private cloud establishes an additional layer of control for users but also imposes increased operational costs.

Broad adoption of cloud computing by financial institutions with varying scalability, security, and compliance needs has increased demand for more flexible approaches. The dichotomy between the use cases for public and private clouds for financial institutions has blurred in practice as CSPs have sought to integrate components of both frameworks.

35. Ibid.
36. NIST SP 800-145.

3.5 DIFFERENT APPROACHES TO ADOPTION

Financial institutions continue to have diverse approaches to cloud use. Their use of SaaS applications, including email, document collaboration, human resources applications, and video conferencing, are now common. However, the use of IaaS and PaaS varied significantly among the firms interviewed for this report. Institutions cited a number of different approaches and desired end-states in their cloud strategy, including migrating to the cloud fully ("all-in"); combining cloud with on-premises architecture ("hybrid); or diversifying reliance on different cloud vendors ("multi-vendor" or "multi-cloud"). Firms interviewed often developed medium- to long-term plans to cloud adoption (e.g., 3–5-year strategic roadmaps). Several institutions also noted that the development of their cloud strategy was accompanied by or helped inform a broader strategic evaluation of their entire IT architecture. Examples of how the firms interviewed were implementing such approaches are described below.

3.5.1 HYBRID APPROACHES

The most common strategy that firms pursued was a hybrid approach, where public cloud deployment continued to be mixed with on-premises or private cloud offerings. This method often involved loading less critical applications to the cloud first to build their in-house understanding and comfort with cloud deployment. It could include migrating sensitive data sets to the cloud, but generally not relying on the cloud for projects that required continuous uptime (e.g., the most critical workloads). In some cases, financial institutions fully integrated cloud deployments to connect with customers as a complete extension or expansion of their on-premises or private cloud capabilities, but such extensions have typically been limited to operations that the financial institution has determined to be less critical. Some firms continue to consider how to develop more technically complex resilience options on the cloud (e.g., as a potential way of rapidly scaling up their infrastructure to meet market needs, or as a backup beyond their primary and secondary data centers), but the development of these options appears to be in very early phases.

3.5.2 MULTI-VENDOR APPROACH

The multi-vendor approach generally refers to a cloud program in which a firm diversifies its exposure to CSPs using multiple vendors. This approach can be divided into two distinct methods: (i) multiple vendors, with each vendor supporting different applications or workloads (referred to as "use cases"); and (ii) multiple vendors supporting the same use cases.

An example of the first instance is when a financial institution uses one CSP for cloud-based video conferencing, another CSP for cloud-based productivity services, and yet another CSP for risk modeling. An example of the second instance is when a financial institution places its customer-facing online banking application on multiple CSPs and

links the applications back to the core platform for processing and recordkeeping. Only a handful of firms interviewed were considering developing this multi-vendor, single-use case deployment for more complex services like IaaS. Doing so would require complex design choices to ensure that data sets were synchronized and application capabilities were the same. It would also require staff with development expertise in multiple cloud environments, as well as accompanying cloud security and risk management expertise. Most firms Treasury interviewed considered multi-vendor, single-use case deployment too technically complex (and, as a result, the accompanying operational risks too high) to even consider developing at this time.

Financial institutions could have a range of reasons to use multiple CSPs. Sometimes firms wanted to diversify services because they evaluated one vendor to have better capabilities for a particular application or workload. Other times, the firm wanted to avoid being locked into a particular vendor. Many firms also minimized using proprietary CSP services and developed their cloud infrastructure around open-source code to reduce risks that they may be effectively locked into a relationship with one CSP. Even with these efforts, swapping complex workloads to another CSP or bringing services in-house was often estimated to take months, if not years to successfully execute in almost all cases.

3.5.3 "ALL-IN" APPROACHES

The firms that most intensively adopted the cloud to retire their existing on-premises IT architecture often focused on service offerings from one vendor because they judged that this approach would reduce operational risks associated with cloud deployment. Monitoring threats, like unauthorized activity, were made easier when all critical information systems were running on the same platform. A single-vendor approach reduced the burden of training staff on the use of multiple platforms. Firms most heavily invested in the cloud stressed their strategy was to reduce their existing data center footprint and retire legacy applications and architecture (i.e., go "all-in" on cloud infrastructure). Several firms expressed that adopting the cloud could help re-focus their organization on technology essential to their businesses.

3.5.4 SELECTING A DEVELOPMENT STRATEGY

Aside from an overall strategy, many firms looked at cloud adoption on a use-case-by-use-case or application-by-application basis, noting that many legacy applications were ill-suited to be placed in a cloud environment without modification. For each application, firms would typically select a development strategy[37] from the following options (which are listed below in order of intensity of change required):

- **Rehost or "Lift and shift"** — moving applications to the cloud as-is.
- **Replatform** — moving applications to the cloud without major changes but taking advantage of the benefits of the cloud environment.
- **Refactor** — modifying applications to be better supported in the cloud environment.

37. Gartner, *Migrating Applications to the Cloud: Rehost, Refactor, Revise, Rebuild, or Replace?* (Dec. 2010), https://www.gartner.com/en/documents/1485116.

- **Rebuild** — rewriting the application from scratch.
- **Replace** — retiring the application and replacing it with a new or existing cloud-native application.

3.6 CLOUD USE BY DEPOSITORY INSTITUTIONS

The cloud strategies of the banks and credit unions Treasury interviewed spanned the broad spectrum of cloud adoption. A small number of depository institutions operate entirely on the public cloud. Some institutions noted that the cloud was necessary to compete with non-depository and fintech firms for reasons including speed to market, cost, and customer experience. Still, other institutions noted an unwillingness to move to the cloud at this time because of challenges related to contracting, skills, or confidence in being able to meet regulatory requirements in a cloud environment.

Depository institutions have started storing sensitive data on the public cloud, from community banks and credit unions to global systemically important banks. Most interviewed institutions generally moved workloads to the private cloud before considering the public cloud. Some depository institutions operated sensitive workloads in the cloud environment (like deposit and loan systems and payments and trade processing). Many banks noted that risk modeling, particularly when utilizing artificial intelligence techniques offered by CSPs, was superior to what they could produce using on-premises architecture.

Depository institutions' exposure to the cloud is also indirect via third parties that also rely on cloud services. Financial institutions noted that many of their third-party suppliers were moving to cloud-based offerings and no longer offering on-premises compatible solutions, forcing a migration to the cloud. Some financial institutions noted it could be easier and more secure to interface with third-party suppliers when they used the same cloud environment.

SECTOR-WIDE TRENDS

According to a survey conducted in 2021 by the ABA, more than 90 percent of surveyed banks stated that they maintain at least some data, applications, or operations in the cloud.[38] Of those surveyed, more than 80 percent indicated they were in the "adoption" or "early adoption" phase with cloud services. Only 5 percent of respondent banks described their cloud use as mature.

According to a May 2022 survey conducted by a CSP, over two-thirds of the surveyed banks want at least 30 percent of their applications and data to be in the cloud in three years.[39] This figure would represent approximately triple the rate of cloud adoption from the time of the survey.[40] Similarly, a 2021 consulting company survey of banks, including North American financial institutions, estimated that an average of 8 percent of all banking

38. ABA *Cloud Computing*.
39. Publicis Sapient in collaboration with GCP, *Future of Cloud in Banking - Report -- How leading banks accelerate digital transformation with cloud* (May 2022).
40. Ibid.

workloads were cloud-based.[41] This same survey indicated 24 percent of respondent banks located in North America had partially migrated core services to the cloud.[42]

3.7 CERTAIN NONBANKS

3.7.1 INVESTMENT ADVISERS, INVESTMENT COMPANIES, BROKER-DEALERS

Larger investment advisors, investment companies, and broker-dealers are adopting cloud computing services to scale operations, build for business continuity needs, and launching products more quickly to market. Some firms started natively in the cloud and have built their entire technology stack in the cloud. Other firms are either in the process of preparing to move to the cloud, piloting workloads in the cloud, or scaling operations in the cloud, typically in an incremental fashion. Still, others have yet to transition to the cloud significantly and are taking a "wait-and-see" approach to gain additional information as cloud computing matures.

Most of these types of financial institutions are not "all-in," nor do they plan to execute a "lift-and-shift" deployment. Rather, they are assessing cloud services as a technology to be deployed where appropriate and not yet for core processing. Some exceptions exist, particularly among smaller institutions with limited IT resources. Smaller institutions tend to use cloud services largely through third-party software providers and managed serviced providers who, in turn, use the larger CSPs.

Lastly, as securities and investment firms make greater use of Artificial Intelligence / Machine Learning (AI/ML), they rely increasingly on cloud services and provisioning to accommodate the large data sets and computing power required for AI/ML.

3.7.2 INSURANCE COMPANIES

Insurance companies are also migrating to the cloud environment for similar reasons. One firm noted the importance of leveraging the cloud for its modernization and improving the customer experience, not simply replicating existing on-premises workloads. This approach entails the development of most, if not all, new applications in the cloud.

Some insurance companies are prioritizing the most dynamic workloads to migrate first to the cloud. Examples of these more high-priority activities include a company's official website or artificial intelligence (AI) platforms that require regular updating, as compared to more static workloads that could continue running on the mainframe. In contrast, others are choosing to migrate all workloads to the cloud to minimize their on-premises footprint. Insurance companies that operate globally are considering adopting cloud across their enterprise, but generally will be more mature in their U.S. operations, partly because of the differences in regulatory requirements.

3.7.3 HOUSING-RELATED ENTITIES

Housing finance entities participating in U.S. mortgage markets by offering single- and multi-family lending, as well as participating in mortgage securitizations and related

41. Accenture Banking Cloud, *What does it mean to be a bank in the cloud*?, Altimeter Volume #1 (2022).
42. Ibid.

products or loan servicing, are also utilizing cloud services. Some housing finance entities have migrated critical business operations to the cloud, though many are at varying degrees of cloud adoption. One basis for cloud adoption is an interest in leveraging machine learning techniques and capabilities for the control environment and managing IT assets. Cloud services adopted by housing finance entities support a range of business activities and internal operations, including IT and cybersecurity management, monitoring, logging, and reporting. Certain entities have implemented an "all-in" approach to the cloud, and others have initiated the migration process but have yet to determine whether a complete transition to the cloud is operationally beneficial and feasible. Through the migration process, however, some firms have ascertained that they could "lift and shift" few of their applications to the cloud. Instead, extensive refactoring is required to complete the transition.

3.7.4 FINANCIAL SECTOR TECHNOLOGY SERVICE PROVIDERS

Several technology service providers that specialize in providing services to financial institutions (such as for core banking and trading software) are also turning to cloud services. They are particularly motivated to reduce costs and technical debt with legacy software in favor of on-demand costs and features desirable to their clients. These technology service providers are also leveraging SaaS applications for business operations (e.g., Office 365, Salesforce), accounting, human resources (HR) software, and high-traffic consumer-facing applications.

Many of these financial sector technology service providers have business models that rely on maintaining service-level agreements (SLAs) with their client financial institutions. The SLAs may specify uptime percentages and recovery time objectives in the event of a disruption of services to their client financial institutions. Therefore, these technology service providers tend to have a low tolerance for network disruptions or outages at their suppliers and sub-contractors. One of the financial sector technology service providers interviewed in connection with this report indicated that in their view, the resiliency/up-time capabilities that CSPs offer the service providers did not always map to, or support, the same level of resiliency/up-time that the financial sector technology service provider offered to its client financial institutions.

Financial sector technology service providers are also motivated to pursue cloud adoption and cloud-native application development to meet the demand of customers who increasingly operate in a cloud environment. This motive is true of the activities that service providers inherit through acquisitions (e.g., fintechs) that are mainly operating in the cloud environment, amounting to a significant portion of companies' existing cloud activities. With these factors combined, many providers Treasury interviewed stated their belief that their migration to the cloud is an inevitability given external trends.

These technology providers have begun integrating cloud services using a variety of adoption strategies and with different long-term goals (e.g., full cloud migration,

hybrid). Some of these service providers have opted to rely heavily on the CSPs' security offerings, and others have emphasized portability as a design consideration. One provider interviewed noted its intention of building its new products natively in the cloud while largely retaining its legacy products (e.g., back-office processing, check imaging) on-premises.

3.8 CRITICAL MARKET INFRASTRUCTURE

FMUs and other entities subject to the SEC's Regulation for Systems Compliance and Integrity (Reg SCI) as well as registered entities subject to the CFTC's System Safeguards Regulations, are also exploring cloud services. Because of the nature of their business, these entities prioritize investment in resiliency measures to ensure near-uninterrupted availability of their services. These entities principally use SaaS applications in the cloud for internal, non-critical purposes (e.g., corporate employee operations, HR systems, Office365, Salesforce), while many core business processes (e.g., clearing, settlement) have remained on-premises. Further, most of these entities are focused on evaluating which of their activities would most benefit from moving to the cloud, not migrating all their operations.

SCI and CFTC registered entities' cloud adoption varies significantly. One entity has used the private cloud to host operations it has determined to be non-critical while it looks to a more phased-in expansion to the public cloud. Another registered entity's failback plan involves maintaining an on-premises data center that could continue its operations for 30 days in the case of a CSP outage. Other registered entities assert that there are more resiliency measures available in the cloud to protect against ransomware attacks than there are on premises. Another registered entity uses the cloud for analytics, regulatory reporting, and systems it determines to be non-critical. One larger registered entity plans to migrate its critical services to the cloud in the next two years after migrating systems not covered under the SEC's Reg SCI. One swap data repository has also transitioned to the cloud, where it now stores all its swap data. Another registered entity has established a partnership with a CSP, intending to consolidate and enhance the various services provided to its customers without the need to rely on multiple vendors.

Domestic and International Regulatory Framework

4.1 U.S. REGULATORY FRAMEWORK AND AUTHORITIES

Financial institutions routinely depend on other financial institutions, financial market infrastructure, common utilities, and a wide network of other third parties to deliver services safely and efficiently to customers. These dependencies, including on cloud services, are often subject to a range of institutional controls and risk management frameworks, as well as regulatory requirements.

FBIIC members have a range of authorities and mandates with respect to financial institutions and their third-party risks. In general terms:

- The FDIC, FRB, and OCC supervise and regulate the safety and soundness of banking institutions and certain related or affiliated entities, and the NCUA does the same for credit unions;
- The SEC and CFTC oversee and regulate key participants in the securities and derivative markets, including broker-dealers, investment companies and advisors, exchanges, clearing entities, and financial market utilities;
- The FHFA has the authority to regulate and supervise Fannie Mae, Freddie Mac, and the Federal Home Loan Banks;
- The CFPB has a range of authorities to regulate consumer protection issues at financial institutions, which can include consumer harm caused by insufficient data protection or security for sensitive information;[43] and,
- The ACSSS, CSBS, NAIC, NASCUS, and NASAA represent state banking, markets, and insurance regulators, which can have a range of authorities over state-regulated entities.

The U.S. financial services regulatory and supervisory regime is generally neutral on the types of technology services that regulated entities use with regard to their operations or the financial services they provide. Applicable federal regulatory requirements[44] place responsibility for effective and appropriate management of technology operations and related risks, such as cybersecurity, on financial institutions, regardless of whether any particular activities or operations are outsourced to third parties. Financial institutions generally have discretion to choose vendors, services, and other aspects of their technology architecture. In certain cases, there are requirements for the financial institution to notify its regulator of a change or planned change to a technology system or the use of a technology service provider.

43. *See e.g.*, CFPB, *Circular 2022-04, Insufficient data protection or security for sensitive consumer information*, (Aug. 11, 2022), available at https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.
44. The focus of this section is on U.S. federal regulatory frameworks. In certain cases, these requirements may also be supplemented by laws, rules, and regulations from state regulatory authorities.

GENERAL REQUIREMENTS

The privacy and disclosure provisions of the Gramm-Leach-Bliley Act (GLBA) generally reflect U.S. policy that financial institutions have an affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic information.[45] These requirements apply to financial institutions, which are generally defined as any institution the business of which is engaging in financial activities, where financial activities are broadly defined and include lending, transferring, investing, or safeguarding money or securities, as well as providing certain insurance and advisory services.[46]

GLBA generally requires financial institutions to notify consumers of the disclosure of their nonpublic personal information (NPI) to nonaffiliated third parties and requires financial institutions to allow consumers to opt-out of such disclosures, subject to certain exceptions.[47] A notable exception to this rule is providing NPI to nonaffiliated third parties that perform services for or functions on behalf of the financial institution. In such cases, the financial institution must disclose the sharing of such information and enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of the information.[48] GLBA also requires the FDIC, FRB, NCUA, OCC, SEC, the Federal Trade Commission, and state insurance regulators to establish appropriate standards for covered financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards to: (i) ensure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[49]

AGENCY-SPECIFIC STANDARDS

U.S. regulators' rules, regulations, and guidance applicable to cybersecurity and third-party risk management of financial institutions can take different forms depending on the issuing agency's statutory authority. For example, the FDIC, FRB, and OCC have issued Interagency Guidelines Establishing Information Security Standards[50] ("Guidelines") pursuant to authorities under GLBA and the Federal Deposit Insurance Act. The Guidelines apply to customer information maintained by or on behalf of entities over which the banking agencies have authority. The Guidelines set forth standards for covered entities when implementing a comprehensive written information security program.[51] Under these

45. 15 U.S.C. § 6801.
46. 15 U.S.C. § 6809; 12 U.S.C. § 1843(k). *See also* 16 C.F.R. § 314.2(h) (a Federal Trade Commission rule setting out examples of entities that are or are not financial institutions).
47. 15 U.S.C. § 6802(a).
48. *Id.*
49. 15 U.S.C. §§ 6801(b), 1805(b). The CFTC is also required, under 7 U.S.C. § 7b-2, to prescribe GLBA regulations for certain entities under its jurisdiction.
50. 12 CFR pt. 30, app. B (OCC); 12 CFR pt. 364, app. B (FDIC); 12 CFR pt. 208, app. D-2, and pt. 225, app. F (FRB). For convenience, example citations to these Guidelines are made to the FDIC version.
51. *See* 12 CFR pt. 364, app. B, § II (FDIC).

Guidelines, information security programs should include administrative, technical, and physical safeguards appropriate to the size and complexity of the entity and the nature and scope of its activities. Under the Guidelines, an institution's information security program should generally be designed to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. Ensure the proper disposal of customer information and consumer information.[52]

The Guidelines also set forth specific standards concerning an institution's oversight of service provider arrangements. These standards include (i) exercising appropriate due diligence in service provider selection, (ii) obligating service providers (by contract) to implement appropriate information security measures that are designed to meet the objectives of the Guidelines, and (iii) ongoing monitoring of the relationships to confirm that the service providers have satisfied their information security obligations (where indicated by the institution's risk assessment). Additionally, the FDIC, FRB, and OCC have each issued third-party risk management guidance and have collectively proposed updated and uniform guidance.[53]

The SEC has implemented Reg SCI for certain entities under its jurisdiction.[54] With respect to securities, Reg SCI sets standards for systems that directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance. SCI Entities are required to, among other things, establish, maintain, and enforce written policies and procedures that are reasonably designed to ensure that these systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets.

Reg SCI requires SCI Entities to maintain business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse, and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption. The SEC has also issued a proposed rule to prohibit registered investment advisors from outsourcing certain services or functions without first meeting minimum requirements.[55]

52. 12 CFR pt. 364, app. B, § II.B (FDIC).
53. *See Proposed Interagency Guidance on Third-Party Relationships: Risk Management*, 86 Fed. Reg. 38182 (July 19, 2021).
54. 17 C.F.R. § 242.1000 *et seq*. SCI entities include self-regulatory organizations, including registered clearing agencies, the registered national securities exchanges, and certain alternative trading systems, plan processors, exempt clearing agencies and competing consolidators of equity market data.
55. *See* SEC, *Outsourcing by Investment Advisers*, 87 Fed. Reg. 68816 (Nov. 16, 2022).

In addition to GLBA rules that apply to certain CFTC-regulated entities,[56] the CFTC has implemented system safeguards requirements for certain other registered entities.[57] Those entities must establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk through the development of appropriate controls and procedures and automated systems that are reliable, secure, and have adequate scalable capacity. In addition, the system safeguards require that those registered entities have business continuity and disaster recovery plans sufficient to enable timely recovery and resumption of operations, generally by the next business day.[58] And for derivatives clearing organizations (DCOs) designated by FSOC to be systemically important, the requirement is resumption of operations two hours following the disruption.[59] Furthermore, if a DCO determines to meet any system safeguards requirement using a contractual arrangement with another DCO or other service provider, the DCO shall retain complete responsibility for any failure to meet related safeguards requirements and the DCO must employ personnel with the expertise necessary to enable it to supervise the service provider's delivery of the services.[60]

EXAMINATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

Subject to the scope of each agency's authorities, FBIIC members' supervision and examination of financial institutions may include a financial institution's technology operations and related risk management programs. Agencies may review a financial institution's governance related to technology and cybersecurity risks, assess the financial institution's risk management program for IT security and resilience, and review the results of tests of relevant response and recovery programs to understand the resiliency of the financial institution's operations and services.[61] For example, the FDIC, FRB, and OCC review whether supervised institutions' third-party relationships and risk management practices are consistent with the safety and soundness of those institutions. Such reviews may also include understanding how a financial institution manages the risks posed by services provided to the institution by third parties.[62]

The Federal Financial Institutions Examination Council (FFIEC),[63] FHFA,[64] and others have issued documents that provide examples of risk management practices that

56. *See* 17 C.F.R. Part 160; *id.* at § 160.30 (providing rules for "[e]very futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, major swap participant, and swap dealer subject to the jurisdiction of the [CFTC]").
57. System safeguards requirements apply to derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories. 17 C.F.R. Parts 37, 38, 39, and 49.
58. 17 C.F.R. § 37.1401(c), 38.1051(d), 39.18(c)(2) and 49.24(d).
59. 17 C.F.R. § 39.34(a).
60. 17 C.F.R. § 39.18(d)(2).
61. For example, in 2021 alone, the FDIC conducted 1,271 specialty examinations for Information Technology and Operations at state nonmember banks, assigning an IT rating using the FFIEC Uniform Rating System for Information Technology. *See* FDIC, *2021 Annual Report* 29, 34, https://www.fdic.gov/about/financial-reports/reports/2021annualreport/2021-arfinal.pdf.
62. This type of review is often referred to as "indirect supervision" of third-party services.
63. *See* FFIEC, *Joint Statement: Security in a Cloud Computing Environment*, https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf; FFIEC, *Information Technology Examination Handbook: Architecture, Infrastructure, and Operations*, https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations.aspx.
64. *See* FHFA, *Cloud Computing Risk Management, AB 2018-04*, https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Cloud-Computing-Risk-Management.aspx.

support the safe and sound use of cloud computing, as well as specific alerts and checklists related to cloud services.[65] Although agencies' rules, guidance, examination practices, and resources may differ, they often draw upon or can be mapped against common standards and frameworks, such as the NIST Cybersecurity Framework, Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO) standards, Center for Internet Security (CIS) Critical Security Controls, and CISA's Cybersecurity Performance Goals.[66] The FHFA also monitors cloud adoption among regulated entities through regular examinations and reviews of entities' technology risk programs.

NOTIFICATION REQUIREMENTS FOR SYSTEMS CHANGES

Several federal financial regulatory agencies require financial institutions to notify the appropriate regulator of changes to their technology systems. For example, U.S. banks are required to provide ex-post notification to their primary federal regulator of the existence of certain types of service relationships.[67] Certain CFTC-registered entities must inform the CFTC of planned changes to automated systems that impact reliability, security, or capacity and planned changes to the registered entities' program of risk analysis and oversight.[68] SCI entities must report quarterly to the SEC on completed, ongoing, and planned material changes to SCI systems and the security of indirect SCI systems.[69]

DIRECT EXAMINATION AND REGULATION OF THIRD-PARTY SERVICES

The FDIC, FRB, and OCC have statutory authority under the Bank Service Company Act (BSCA)[70] to examine and regulate the performance of certain services provided by third-party providers to supervised financial institutions to the same extent as if a supervised depository institution performed such services itself on its own premises.[71] This authority does not extend to services provided to entities not covered under the BSCA or to the service provider more generally. The BSCA covers banking services, such as computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions, as well as activities such as data processing.[72] In 2022, the FDIC, FRB, and OCC, by regulation, established a requirement on service providers that

65. *See, e.g.*, SEC, *Risk Alert: Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features* (May 23, 2019), https://www.sec.gov/ocie/announcement/risk-alert-network-storage; North American Securities Administrators Association, *Cybersecurity Checklist for Investment Advisors*, (2017), https://www.nasaa.org/wp-content/uploads/2018/10/NASAA-Cybersecurity-Checklist.pdf.
66. For example, the FFIEC released a mapping of its cybersecurity assessment tool to the NIST cybersecurity framework. FFIEC, *Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework*, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf.
67. 12 U.S.C. § 1867(c)(2). ("the depository institution shall notify each such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.") The scope of this Bank Service Company Act requirement is discussed further below. *See also* 12 U.S.C. § 1464(d)(7)(D) (setting out similar requirements for savings associations).
68. 17 CFR § 37.1401(f), 38.1051(f), 39.18(h)(1)–(2) and 49.24(h).
69. 17 CFR § 242.1003.
70. 12 U.S.C. § 1861 *et seq*. *See also* 12 U.S.C. § 1464(d)(7)(D).
71. 12 U.S.C. § 1867(c).
72. *See* 12 U.S.C. §§ 1863 and 1864.

fall within the scope of the BSCA to notify their affected client financial institutions in the event a computer-security incident has materially disrupted or degraded or is reasonably likely to materially disrupt or degrade covered services to such customers for four or more hours.[73]

Whether or not the performance of a particular service provided by a service provider is examined (as well as the frequency and priority of any such examinations) is based on a case-by-case analysis of the criticality of the service, the number of financial institutions under contract with the service provider, and the inherent risk that the service may present to client financial institutions, among other considerations. Each of these examinations results in an examination report, a portion of which is available, either automatically or upon request, to financial institution clients of the service provider.[74]

Other federal financial regulatory agencies do not have examination and regulatory authority over services provided by third parties similar to the authority provided to the FDIC, FRB, and OCC by the BSCA. Nonetheless, there may be circumstances in which such agencies can conduct tailored oversight of third-party services, such as cloud services, provided to their regulated entities. Title VIII of the Dodd-Frank Act also allows supervisory agencies of designated financial market utilities (DFMUs)—currently the FRB, SEC, and CFTC—to examine the provision of a service provided by another entity when such a service is "integral" to the operation of the DFMU.[75] To address risks related to the Y2K transition, the NCUA once had broad, temporary examination authority over third-party providers to credit unions similar to that provided in the BSCA, but this authority expired in 2001.[76] The Financial Stability Oversight Council has recommended that both the FHFA and NCUA be provided adequate examination and enforcement powers to oversee third-party service providers.[77]

Apart from statutory authority, contracts with third-party service providers may cover audit requests by financial institutions and their regulators.[78] However, some FBIIC members report that this means of gathering information may not be as effective as statutory authority.

INSURANCE SECTOR

In the United States, the business of insurance is primarily regulated by state law, both in terms of solvency and market conduct. Regulation at the state level frequently follows model laws and regulations adopted by NAIC. Early in 2017, the New York Department of

73. 12 CFR 53.4 (OCC); 12 CFR 225.303 (FRB); 12 CFR 304.24 (FDIC). The compliance date of this final rule was May 1, 2022.
74. See FFIEC, Information Technology Examination Handbook: Supervision of Technology Service Providers, https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/risk-based-supervision/roe-distribution.aspx.
75. 12 U.S.C § 5466 (b) ("the Supervisory Agency may examine whether the provision of that service is in compliance with applicable law, rules, orders, and standards to the same extent as if the designated financial market utility were performing the service on its own premises").
76. NCUA, *Third Party Vendor Authority* (Mar. 2022), https://www.ncua.gov/files/publications/regulation-supervision/third-party-vendor-authority.pdf.
77. FSOC, *2022 Annual Report* 72, https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf
78. See FFIEC, Information Technology Examination Handbook: Outsourcing Technology Services, 11–15, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/contract-issues.aspx.

Financial Services finalized its Cybersecurity Regulation, which includes requirements related to regulated entities' use of third-party service providers. Later that year, the NAIC adopted a similar Insurance Data Security Model Law,[79] which, when incorporated into law by individual states, establishes standards for data security and for the investigation of and notification to the State Insurance Commissioner of a cybersecurity event. In general, the model law requires an insurer to develop, implement, and maintain a comprehensive, written information security program that evolves from its risk assessment, including its use of third parties, for the protection of data and systems, and report third-party arrangements to the board of directors. Over twenty states have adopted some form of the NAIC model law.

ROLE OF U.S. TREASURY AND SECTOR-WIDE COORDINATION EFFORTS.

Presidential Policy Directive 21 designates Treasury as the Sector Risk Management Agency (SRMA) for the financial services sector. In carrying out its general responsibilities as an SRMA, Treasury is required to coordinate with the Department of Homeland Security and, as appropriate, other relevant Federal departments and agencies; collaborate with critical infrastructure owners and operators within the financial sector; and coordinate with independent regulatory agencies, and state, local, Tribal, and territorial entities, as appropriate. Treasury and each SRMA leverage their knowledge and expertise to:

- Support sector risk management in coordination with CISA;
- Assess sector risk in coordination with CISA, including identifying, assessing, and prioritizing risks within the sector;
- Support sector coordination, including serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities;
- Facilitate, in coordination with CISA, the sharing of information regarding physical security and cybersecurity threats within the sector;
- Support incident management, including supporting, in coordination with CISA, incident management and restoration efforts during or following a security incident; and,
- Contribute to emergency preparedness efforts, including coordinating with critical infrastructure owners and operators within the sector and CISA in developing planning documents for coordinated action in the event of a natural disaster, an act of terrorism, or other disaster or emergency.

One of the key mechanisms for coordination in the financial sector is the FBIIC. Staff from FBIIC member organizations work on operational and tactical issues related to critical infrastructure matters, including cybersecurity, within the financial services industry. The senior leaders of FBIIC are the principals from each member organization. This group meets tri-annually to provide strategic, policy-level direction to FBIIC's work. Topics

79. NAIC, *Insurance Data Security Model Law* (2017), https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf.

include enhancing information-sharing, promoting coordination on incident-response planning, and identifying best practices for cybersecurity controls at financial institutions.

Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) works closely with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents.

4.2 INTERNATIONAL APPROACHES

U.S.-based cloud services are increasingly used in foreign financial sectors[80] and by U.S. financial institutions operating abroad. As a result, international regulatory frameworks, and specific requirements from foreign jurisdictions, can significantly influence the services CSPs provide and how they engage with financial institutions and authorities. Foreign approaches to regulating cloud and other types of third-party services also provide a comparative reference for the U.S.

Over the last twenty years, international financial sector standard-setting bodies[81] (SSBs) and individual foreign regulators have established requirements and guidance on outsourcing, third-party risk management, and operational risk largely similar to the approaches taken by U.S. regulatory agencies. Several FBIIC members are active participants within the Financial Stability Board (FSB) and SSBs. Member agencies also have been leaders in exchanging views with foreign regulators on operational resilience and third-party providers, including cloud services.

The broader entry of technology companies and new financial technology companies into the financial services sector has partly motivated international regulatory scrutiny of public cloud services. Concerns over concentration risk and the lack of regulatory authority over third-party service providers that may be critical to foreign financial sectors have led to new legislative proposals for enhanced regulation of third-party service providers, including in the European Union and the United Kingdom.

INTERNATIONAL POLICY DEVELOPMENT

In 2005, the Joint Forum, formed jointly by the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS), issued outsourcing guidance for financial services. The guidance, *inter alia*, affirms that responsibility for compliance remains with the regulated financial entity, recommends contingency planning for

80. Cloud Security Alliance, *Cloud Usage in the Financial Services Sector* (2020); Institute of International Finance, *Cloud Adoption and Regulation in Asia-Pacific Financial Services* (Nov. 2021) https://www.iif.com/portals/0/Files/content/Innovation/11_10_2021_cloud_asia_pacific.pdf.

81. The international standard-setting bodies in the financial sector include the BCBS, IOSCO, IAIS, and the Committee on Payments and Market Infrastructures. In 2009, the G20 created the Financial Stability Board (FSB) to oversee the development of standards. The FSB is tasked with monitoring financial stability, coordinating between the standard-setting bodies, and undertaking tasks as requested by the G20.

financial entities and their providers, and notes the importance of monitoring for potential risks posed when multiple regulated entities' outsourced activities are concentrated in a limited number of service providers.[82] Each of the SSBs has continued to build upon and refine the approach outlined in 2005 by the Joint Forum. For example, IOSCO revised its *Principles on Outsourcing*[83] in 2021, combining and updating expectations issued by the Joint Forum and separately by IOSCO in 2009. And the Committee on Payments and Market Infrastructures and IOSCO jointly issued the Principles for Financial Market Infrastructure (PFMI) in 2012, which includes Annex F: *Oversight expectations applicable to critical service providers.*[84] Expectations included effective risk identification and management, information security practices and policies, reliability and resilience, technology planning, and communication with users. The IAIS Operational Resilience Task Force (ORTF) was formed in 2020 to develop supervisory supporting materials on issues related to cyber resilience, including implications of cyber risks from outsourcing technology services to TSPs, and to review best practices from the industry and supervisors. The ORTF is currently drafting an Issues Paper on Operational Resilience that is expected to be finalized in 2023, and which will address outsourcing critical IT functions, among other issues.

DEVELOPMENTS AT THE FINANCIAL STABILITY BOARD

The FSB first identified third-party provider oversight as an area meriting further attention in 2017,[85] and published two related reports in 2019. The first outlines the benefits and risks of cloud service utilization[86] and the second reviews standards and practices applicable to third-party risk, including guidelines for the use of cloud services.[87] Based on interviews with public- and private-sector entities, public sources, proprietary data, and a survey, the FSB concluded that "there are no immediate financial stability risks stemming from the use of cloud services by [financial institutions]."[88] Since then, as cloud use by the financial system has accelerated globally, foreign regulators have continued to focus on cloud adoption as a primary reason for establishing new regulatory frameworks to oversee technology providers they determine to be critical.

In November 2020, the FSB published a discussion paper that, among other things, outlined financial authorities' views regarding the "indirect" model of supervision of third-party risk.[89] An FSB survey revealed that the direct third-party examination authority was relatively rare. Issues identified by FSB members included:

82. The Joint Forum, *Outsourcing in Financial Services* (Feb. 2005), https://www.bis.org/publ/joint12.pdf.
83. IOSCO, *Principles on Outsourcing* (Oct. 2021), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.
84. Annex F of the PFMI was primarily written to cover the activities of SWIFT, a financial sector specific technology provider that performs necessary functions for the cross-border payments system.
85. FSB, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* (June 2017), https://www.fsb.org/2017/06/financial-stability-implications-from-fintech/.
86. FSB, *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications* (Feb. 2019), https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/.
87. FSB, *Third-Party Dependencies in Cloud Services: Considerations on Financial Stability Implications* (Dec. 2019), https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/.
88. Ibid.
89. FSB, *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* (Nov. 2020), https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/.

- Practical limitations on financial institutions' abilities to manage the risks in their outsourcing and third-party agreements (including risks in the wider supply chain of third-party providers, i.e., fourth and fifth parties);
- Limitations on regulators' abilities to effectively oversee financial institutions' outsourcing and third-party arrangements in a cross-border context; and,
- Challenges in identifying, monitoring, and managing potential systemic risks related to financial institutions' use of outsourcing and third-party arrangements, in particular, due to concentration on the provision of third-party services and a lack of relevant information.

To address these supervisory challenges, the FSB is working with its members and the SSBs to develop a toolkit for financial institutions to assist in the identification and risk management of critical third-party services for public release in 2023. The toolkit will also provide tools to financial authorities in their oversight of these risks.

DEVELOPMENTS AT THE G7

Established in November 2015, the G7 Cyber Expert Group (CEG) meets regularly to identify the leading cyber security risks in the financial sector and to propose actions to be taken in this area. U.S. Treasury and the Bank of England chair the CEG. While not an SSB, the CEG nonetheless helps drive the development of international cybersecurity policies across the G7 (and beyond) through its publication of "fundamental elements." Notably, the group published the "G7 Fundamental Elements of Cybersecurity for the Financial Sector" in October 2016 and the "G7 Fundamental Elements for Effective Assessment of Cybersecurity" in October 2017.

Building on these publications, the CEG published the "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" in 2018, with an update in October 2022.[90] The fundamental elements stress the importance of financial institutions' governance and risk management processes, as well as their strategy to identify third parties and the criticality of their services to the financial institution. It also notes the importance of due diligence, contract structuring, ongoing monitoring, and contingency planning. The fundamental elements also note the need for relevant authorities to identify and assess potential systemic risks and encourage efforts to improve information sharing and coordinate across sectors regarding cyber risks stemming from third parties. The 2022 update included a new element, noting that third parties should make information available to facilitate financial institutions' management of cyber risk.

FOREIGN REGULATION OF CLOUD SERVICES

Foreign jurisdictions have promulgated a diverse array of guidelines and requirements applicable to the use of cloud services. These regulations can potentially affect a range of U.S. financial sector policy interests concerning cloud services. First, foreign regulatory

90. G7 CEG, *G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* (Oct. 2022), https://www.bundesbank.de/resource/blob/624828/91c47c36b53ca366e2950881591de0ab/mL/2022-10-13-g7-fundamental-elements-cybersecurity-data.pdf.

frameworks directly impact how U.S. financial institutions adopt cloud services cross-border or globally. These requirements drive strategic decision-making around technology architecture at many large, international financial institutions, including U.S. banks and insurance companies. Many financial institutions report significant difficulties in adopting cloud services consistently across jurisdictions. Second, cloud services are generally offered on a global basis. To streamline technology development and risk management, and to cater to an international audience, the practice of many cloud providers is to promote consistency in their global cloud offerings. A feature necessary for a local requirement is often replicated in multiple regions. Foreign financial sector regulations and requirements can therefore affect the services used by U.S. financial institutions and, in some cases, potentially services provided to all customers.

Several jurisdictions (notably, China) essentially prohibit the use of U.S.-based cloud services through prescriptive requirements such as requirements to store data locally or use only local providers. These restrictive approaches are in opposition to the favored approach by the U.S, which pursues a policy agenda supportive of cross-border data flows.[91] Foreign jurisdictions may impose prescriptive requirements limiting cross-border data flows for a wide range of policy reasons, including for data privacy or concerns that financial institutions and regulators may not be able to access data held abroad; however, these measures are often unnecessarily restrictive and antithetical to the technology architecture of the cloud. Even without explicit prohibitions, obtaining regulatory approvals or non-objections for technology adoption, particularly involving cross-border services, can be difficult. In response to some of these restrictive policies, financial industry trade associations have advocated for global principles for regulating public cloud services,[92] arguing that regulators should recognize the benefits of public cloud, support harmonizing public cloud requirements and the free movement of data, among other principles.

More like-minded authorities, including within the G7, have generally pursued regulatory frameworks that are broadly similar to the U.S. regulatory framework. However, in some cases, U.S. financial institutions and cloud service providers report pressure to localize data to meet local requirements, as well as difficulties in navigating the variations in regulatory requirements. Some jurisdictions closely aligned with the U.S. are also looking at expanding their regulatory authorities over third-party providers, either by expanding the scope of their relevant critical infrastructure legislation or seeking direct authority for financial regulators to oversee certain critical third-party services.

91. U.S. Treasury and Monetary Authority of Singapore, *United States – Singapore Joint Statement on Financial Services Data Connectivity* (Feb. 2020), https://home.treasury.gov/news/press-releases/sm899.
92. ASIFMA, *Proposed ASIFMA Principles for Public Cloud Regulation* (Mar. 2021), https://www.asifma.org/wp-content/uploads/2021/03/final-proposed-asifma-principles-for-public-cloud-regulation.pdf.

For example, Australia adopted the Security of Critical Infrastructure Act 2018,[93] which was designed to address national security risks associated with Australia's critical infrastructure (including by foreign providers). The Act was amended in 2021 and 2022 to apply to 11 economic sectors, including data storage and processing. The act requires mandatory cyber incident reporting, a register of critical infrastructure assets, enhanced cyber security obligations, and adopting a critical infrastructure risk management program for critical infrastructure assets. It also has a smaller subset of critical infrastructure called Systems of National Significance to which are subject to enhanced cyber security obligations. The Act also grants the Australian Department of Home Affairs the power to obtain information directly from owners and operators of critical infrastructure assets and allows the Australian Government to authorize directions and interventions during a cyber incident. In 2018, the Australian Prudential Regulatory Authority (APRA) released an information paper on outsourcing involving cloud services.[94] The report identifies three risk categories into which cloud usage typically falls — low, heightened, and extreme inherent risk — and highlights key issues that financial institutions must consider as part of their risk assessment. And under APRA's outsourcing guidelines, APRA-regulated entities must notify APRA after entering into a material outsourcing agreement. Regulated entities must consult with APRA before entering into an outsourcing arrangement involving a material business activity where offshoring is involved.

In December 2022, the European Union (EU) finalized the Digital Operational Resilience Act (DORA), which will subject regulated financial entities to a set of rules on IT and third-party risk management, regulatory reporting requirements for major IT-related incidents, and requirements for financial entities to conduct penetration testing. In addition, DORA brings critical ICT third-party service providers under an oversight framework. The legislation was informed by recommendations by European Supervisory Authorities, which have noted acute concern with concentration risk associated with CSPs.[95] The oversight framework includes a regulatory structure for critical third-party service providers where one of the three European Supervisory Authorities (ESAs) will serve as the lead overseer. The design of the oversight framework also foresees an Oversight Forum that will support the work of the lead overseers, a Joint Oversight Network that will strengthen the coordination among the lead overseers, and joint examination teams that will assist lead overseers in conducting the necessary investigations and inspections. Each oversight forum for a critical third-party service provider will include representatives from the other ESAs and competent authorities in each Member State (e.g., national central banks). Representatives from national competent authorities under the EU's Network and Information Security Directive would also participate where appropriate.

93. Australian Government Department of Home Affairs, *Security of Critical Infrastructure Act 2018* (2021), https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018.
94. APRA, *Outsourcing Involving Cloud Computing* Services (Sept. 2018) https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf.
95. EBA, ESMA, and EOIPA, *ESAs Publish Joint Advice on Information and Communication Technology Risk Management and Cybersecurity* (Apr. 2019), https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk.

Under DORA, the EU will designate IT third-party service providers as "critical," based on, among other factors, the systemic impact on the provision of financial services if the relevant provider faces a large-scale operational failure. The lead overseer would be authorized to conduct investigations and onsite and offsite inspections, including on premises located in non-EU countries, impose penalties for non-compliance with access and information requests, and issue recommendations. The legislation allows a company to contest designation by submitting a reasoned statement containing any relevant information for the assessment related to its identification. DORA directs the lead overseer to minimize, to the extent possible, the risk of oversight activities disrupting services provided to customers outside of the financial sector. A critical third-party service provider can provide information regarding the expected impact of oversight. DORA also authorizes the ESAs to establish administrative arrangements with regulators in non-EU countries to foster international cooperation on third-party risk.

The United Kingdom (UK) is also considering legislative authority to subject critical third-party services to a framework of regulatory standards and testing developed by financial regulators. The UK's Financial Policy Committee noted that "the increasing reliance by the financial system on critical third parties), including cloud service providers, can bring benefits to the financial sector, including improved operational resilience.However, the increasing criticality of the services that critical third parties provide, alongside concentration in a small number of providers, pose a threat to financial stability in the absence of greater direct regulatory oversight."[96] And in 2021, the International Monetary Fund recommended that the UK supervisory authorities seek additional statutory powers to review and examine the resilience of all critical services (including, but not limited to, cloud services) that third parties provide to regulated firms.[97] In July 2022, the Bank of England, the Prudential Regulatory Authority, and the Financial Conduct Authority published a discussion paper on how such a framework could operate.[98] Designation by His Majesty's Treasury under this framework would recognize "the systemic impact that the disruption or failure of the services that a particular third party provides to firms and FMIs could have on the stability of, or confidence in the UK financial system."[99] Based on current proposals, designated critical third parties would need to ensure that their services to UK financial institutions met minimum resilience standards and test the resilience of these services.

96. UK Financial Policy Committee, *Financial Policy Summary and Record - October 2021* (Oct. 2021), https://www.bankofengland.co.uk/financial-policy-summary-and-record/2021/october-2021.
97. International Monetary Fund, *United Kingdom: Financial Sector Assessment Program-Financial System Stability Assessment* (Feb 2022), https://www.imf.org/en/Publications/CR/Issues/2022/02/22/United-Kingdom-Financial-Sector-Assessment-Program-Financial-System-Stability-Assessment-513442
98. BoE, PRA, FCA, *Operational resilience: Critical third parties to the UK financial sector*, Discussion Paper (July 2022), https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector.
99. Ibid.

U.S. CRITICAL PROVIDERS DIALOGUE

In response to increasing international interest, in May 2022, Treasury and the Federal Reserve Board launched an ongoing multilateral regulatory dialogue among foreign counterparts to discuss cooperation around critical services to the financial sector. The "Critical Providers Dialogue" includes discussion among the parties on regulatory approaches to critical third-party providers, including certain cloud services use cases. This dialogue is designed to complement multilateral work at the G7 CEG and FSB as well as bilateral discussions, such as at the U.S.-EU Joint Financial Regulatory Forum and U.S.-UK Financial Regulatory Working Group.

Financial Institution Practices when Adopting Cloud Services

5.1 RISK MANAGEMENT AND OPERATIONAL RESILIENCE

The financial services sector primarily addresses potential risks of third-party services through risk management practices of individual financial institutions. This section summarizes the steps U.S. financial institutions may generally take when selecting and onboarding different cloud services.[100]

As part of typical processes, a financial institution will determine whether its planned use of cloud services is consistent with its internal policies and is designed to result in the safe and sound operation of the financial institution, the security and confidentiality of its data, and compliance with applicable laws and regulations. The financial institution generally will (1) conduct risk-based due diligence on the CSP and service and (2) establish a range of internal and external (within the cloud environment) security and resilience controls, configurations, and monitoring for the cloud services. In many cases, financial institutions may follow or repurpose as, according to their needs, sector-agnostic approaches such as those outlined by NIST (e.g., NIST SP 500-291 *Cloud Computing Standards Roadmap or* SP 500-332 *Cloud Federation Reference Architecture)* or financial sector-specific approaches, like the Cyber Risk Institute's "Cloud Profile."[101]

A crucial element of a financial institution's mitigation of risk from operational disruption of a CSP is a comprehensive risk management and oversight program for its third-party relationships. The robustness of the third-party risk management and oversight program will vary depending on the function or criticality of the activity supported by a third party. Risk management programs generally include initial due diligence and ongoing monitoring of the third party, including evaluation of performance metrics, security, and other risk controls, disaster recovery plans of the third party, and other alternatives for the financial institution to address operational disruptions of the third party. For example, a financial institution will often evaluate the technology infrastructure of a CSP and the cloud service to consider if it is capable of supporting the financial institution's approach to maintaining operational resilience.

Financial institutions typically conduct due diligence consistent with their internal risk management framework, risk appetite, and regulatory expectations. The depth of due diligence review is generally commensurate with the risk and complexity of the relationship. Due diligence involves reviewing the service provider's capabilities (both operational and financial) to meet the terms of the proposed service engagement and satisfy the risk management standards of the financial institution. The financial institution will also review specific aspects more intensively based on the importance of the service.

100. This section is meant to provide the reader with a general understanding and does not address all steps financial institutions may take. It is not meant to serve as guidance to financial institutions.
101. Cyber Risk Institute, Cloud Security Alliance, Bank Policy Institute, *CRI Announces Completion of Cloud Profile Extension* (Apr. 2022) https://cyberriskinstitute.org/cri-announces-completion-of-cloud-profile-extension/.

For example, if redundancy is critical to the proposed service, a financial institution will evaluate the CSP's capabilities for business resumption and resilience for the purchased cloud services. Among other factors, a financial institution may be looking to assess whether redundancy capabilities of a service are compatible with its own standards and continuity plans, and to determine whether to purchase additional services offered by the CSP for added redundancy.

Third-party assurance reviews, such as service organization controls (SOC) reviews, penetration tests, and vulnerability assessments, can assist financial institutions in understanding a CSP's control environment and its ability to meet a financial institution's control expectations (e.g., compliance with applicable laws and regulations). One of the most common third-party service provider audits are SOC2 reports, conducted under the American Institute of Certified Public Accountants standards for assessing service organizations.[102] SOC2 reports involve an evaluation of the security, availability, processing integrity, confidentiality, or privacy of information and systems across an entire entity, of a particular subsidiary or operating unit, or for a particular function. The SOC2 report can be a type I, a point in time assessment largely based on documented controls, or type II, a sustained observation of a period in time. Typically, CSPs will offer options within the contract that will allow the financial institutions to receive SOC reports or additional reports or evidence for an additional fee. Some financial institutions Treasury interviewed indicated that most CSPs provide SOC2 audit reports at least annually. SOC2 engagements are designed to be flexible and do not prescribe specific controls. This flexibility could be seen as a drawback that limits the independence and utility of the engagement. Some financial institutions Treasury interviewed noted that SOC2 reports were helpful but not sufficient for understanding the control environment and potential security risks for particular services.

A financial institution will also review and rely upon certain security and resilience controls maintained by the CSP. Comprehensive risk management processes typically include requirements for specific language in its contract and SLAs, including those established with the CSPs to ensure clarity regarding the CSP's commitment to specific security and resilience controls for the cloud service. Internal policy and procedures documents often reflect many aspects of the firm's decisions regarding security and resilience controls of a particular cloud service.

5.2 DEPLOYMENT AND CONFIGURATION

To use cloud services, a financial institution establishes and manages a range of communication channels between the CSP and the financial institution's on-premises IT systems. These communication channels align data between the cloud and the on-premises IT systems, allow the financial institution to access the services provided at the CSP, such as computing and data storage, and provide the financial institution with access to an interface for managing the cloud services. Options for these communication

102. Association of International Certified Professional Accountants, *System and Organization Controls: SOC Suite of Services* (Accessed on Nov. 2022), https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.

channels include encrypted communications over the public internet, APIs, and private networks. Malicious actors can exploit improperly secured or configured communication channels, resulting in compromised data or unavailability of the financial institution's services or the cloud services.

CSPs often provide a baseline level of resilience for a contracted cloud service, such as commitments to performance metrics and up-time status in the SLAs with clients. But the financial institution must ultimately make choices in both design and configuration to achieve its preferred balance of security, capabilities, resilience, and cost. A financial institution may take advantage of cloud service configuration options offered by the CSP that can provide a higher operational resilience. These options may include:

- SLAs for increased resilience/up-time. Some CSPs may provide the financial institution with the option of an additional or enhanced level of service availability or uptime, or CSP-provided monetary compensation if the desired service availability is not achieved. The financial institution's contract or SLA with the CSP may reflect these provisions. The availability of increased uptime options from a CSP may vary depending on the CSP and the particular cloud service.
- Multiple data centers within a single CSP region. The CSP may allow the financial institution to maintain its applications and data in multiple, geographically dispersed data centers located in a single region of the CSP. These multiple data centers can provide increased resilience for the financial institution from local operational disruptions that could affect a single data center, such as natural disasters, power supply interruptions, or fires.
- Multiple Regions from the same CSP. Depending on the service model, a financial institution might elect to locate its applications in two different regions of the same CSP. There are variations to this approach, including 'multi-master' or 'active-active' configurations that can recover nearly instantaneously from the failure of a single region without user visibility degradation of performance or loss of data. There can be challenges with the multi-region approach, including costs, staff resources, latency, and lack of similar services in different regions of the same CSP.

With IaaS, clients design significant elements of their control environment.[103] At the financial institution level, controls can include the financial institution's monitoring of performance data provided by the CSP, as well as its configuration of certain aspects of the cloud services within the CSP's environment, such as selecting multi-factor authentication to secure its users' access to cloud features. Even with SaaS configurations, determining appropriate user access rights is the responsibility of the client and not the cloud provider. Setup of security controls and user access rights is among the most important aspects of securing data and workloads in the cloud environment.

103. See Section 3.3 for a more complete explanation of the shared responsibility and its application to IaaS, PaaS, and SaaS. For example, with IaaS, CSPs secure IT hardware and set physical controls, and the client sets controls for the operating systems and applications placed in the cloud environment.

A financial institution may also seek to reduce its long-term reliance on the cloud services of a CSP by designing its applications and data for portability to another CSP. For certain services, particularly IaaS, containerization functionality can support the portability of applications from one CSP to another CSP. The potential for portability and the complexity of managing the portability will vary for different types of services.

While financial institutions have considered portability design in cloud deployments as a means to reduce longer-term dependencies, nearly all of the financial institutions interviewed cautioned that this was not technically feasible as a means to mitigate short-term disruptions in more complex services. Financial institutions also may consider the potential to bring back services to an on-premises environment, but this brings its own set of similar and different challenges (like attempting to develop applications that can work on both a cloud and non-cloud environment, which could require compromises in functionality.)

5.3 MONITORING, AUDITING, AND TESTING

Financial institutions also implement monitoring controls to avoid reliance on historical point-in-time assessments and to execute their security and risk management responsibilities. These controls include using dashboards and logging capabilities offered by CSPs, or a financial institution's own customized, compatible solutions to monitor operational performance and security threats.

Financial institutions may also seek to audit or test operational or security capabilities offered by the CSP. A financial institution can use its internal auditors or engage a third party to conduct regular audits and tests of operational or security controls, such as access management controls and system configuration, commensurate with the risks associated with cloud services. It is also an increasingly common practice that cloud contracts with financial institutions allow for audit by the financial institution, its designee, or its regulator. Some industry clients have also combined their resources to conduct or hire auditors to conduct "pooled" audits. These audit rights, however, are usually subject to a fee-based arrangement for the time and materials associated with ad-hoc requests for information.

Additionally, CSPs regularly refresh their independent audits and certifications, such as SOC reviews. Financial institutions can review these reports to understand how the control environment may be changing at the CSP and better scope their own reviews over time.

Financial institutions may also test capabilities associated with cloud services. For example, several financial institutions Treasury interviewed relayed that they had successfully tested certain backup capabilities related to their cloud deployment.

Challenges with the Financial Sector's Use of Cloud Services

Through the development of this report, Treasury identified several challenges associated with greater cloud adoption by U.S. financial institutions. The challenges cut across multiple use cases, CSPs, and financial institutions.

6.1 INSUFFICIENT TRANSPARENCY TO SUPPORT DUE DILIGENCE AND MONITORING BY FINANCIAL INSTITUTIONS

As noted in Section 5, financial institutions require initial and ongoing information from CSPs to understand the potential risks of their use of cloud services and to support the selection and implementation of mitigating controls. Typical risk management practices in the financial services sector preclude a financial institution from solely relying on contractual commitments or vendor assurance without review or independent verification. Insufficient information from a CSP can weaken an individual financial institution's risk management capabilities. Treasury encountered a range of views on the sufficiency of information from CSPs to inform financial institution risk management. Early adopters and financial institutions with public and prominent relationships were generally more satisfied than others. At the same time, it was a commonly held view among many U.S. financial institutions that Treasury interviewed, as well as industry stakeholders and academics, that existing CSPs' efforts did not fully satisfy financial institution risk management needs. Issues they noted included the following:

- Some financial institutions did not have transparency on how many data centers they were relying on until an incident occurred at the CSP.
- Some financial institutions relayed instances where they thought inconsistency in the documentation for services made use of cloud services more challenging.
- Some due diligence or monitoring requests could not be satisfied with written documentation for risk management purposes, e.g., actual testing results of security controls.
- Some financial institutions would like to obtain information on how CSPs identify and address pervasive security threats to the cloud environment.
- Some financial institutions expressed concern that they did not fully understand the internal dependencies within the cloud environment associated with particular cloud services, e.g., dependencies from other cloud services or fourth parties.
- Some financial institution stakeholders viewed communication from CSPs around operational and cyber incidents as an area that all invested parties could improve.
- While the majority of the focus by financial institutions was related to information associated with IaaS and PaaS, some financial institutions noted transparency challenges with SaaS offerings.

- Some financial institutions not yet directly using public cloud services expressed uncertainty and concern regarding how CSPs would control access to client data, including with respect to CSPs' third-party contractors, and viewed such unknowns as impediments to adoption.
- Smaller financial institutions, in particular, noted the challenges of conducting due diligence on the universe of vendors they rely on given resource constraints.

A wide range of industry and public sector stakeholders interviewed by Treasury conveyed that the major U.S.-based IaaS CSPs are continuing to make progress in addressing the regulatory and risk management needs of their financial institution clients.

However, risks associated with third-party services have become more difficult to measure due to several factors, including by way of "nth party" dependencies. CSPs provide services to many other third-party service providers that a financial institution may rely on, and also use many sub-contractors, creating indirect dependencies for financial institutions that are more difficult to assess.

Some CSPs that Treasury interviewed noted their skepticism around the value of certain requests from their financial institution clients. They argued that recurring physical data center audits often provided little additional security assurance and were challenging to accommodate at scale given the need to maintain physical and data security for the shared tenant environment. Treasury believes that further efforts are needed to achieve the right balance of information sharing between CSPs and financial institutions, which might benefit both groups in terms of efficiency and effectiveness.

6.2 GAPS IN HUMAN CAPITAL AND TOOLS TO SECURELY DEPLOY CLOUD SERVICES

The success of the shared responsibility model ultimately relies on both CSPs and their financial institution clients to each take on tasks to secure the overall environment without either party having full visibility over risks and controls. Financial institutions are generally separated from the security of the underlying cloud environment, and CSPs generally have limited insight into customer activities. Risks can be idiosyncratic to the user: most publicly reported incidents with the cloud have been specific to choices at the client level. As discussed in Section 5, cloud services can be highly resilient and feature security capabilities unavailable in an on-premises environment, but only if configured with that intention. To be effective, the shared responsibility model relies on clients having the expertise, tools, and information necessary to execute their responsibilities and to ensure the contracted cloud service reflects their desired risk tolerance.

MISCONFIGURATION RISKS

Industry research most often cites "misconfiguration" by users as the most common cause of data breaches.[104] For example, prosecutors stated that the individual behind a major incident in 2019 scanned for common misconfigurations among AWS clients to identify potential victims.[105] Although the incident itself involved many complex factors in addition to the misconfiguration issue, the perpetrator of this incident identified 30 similar misconfigurations that they were able to exploit to steal data and illicitly install cryptocurrency mining software, showing that exploitation of common misconfigurations can be easily replicated across a cloud service's customers. Clients can also misconfigure PaaS and SaaS applications through inappropriate user access and a failure to monitor activity, but IaaS can be misconfigured at every level, from design to access to implementation. Once malicious actors see a vulnerability, they will scan for other customers to exploit. Customers that make similar misconfiguration errors can be exploited at scale.

Treasury identified two factors that can make the shared responsibility model less effective. First, the available talent pool to financial institutions to support these activities is well below demand, presenting a potential barrier to entry for financial institutions seeking to adopt cloud services or to maintain appropriate staff for their current needs. Second, many financial institutions reported technical challenges associated with cloud service features and tools to manage cloud services.

As one major report concluded, "Shared responsibility masks the uneven maturity of organizations and technologies on the user side of that shared line, producing much more of a zigzag than a clean line of responsibility."[106] This challenge is particularly acute for small and medium-sized financial institutions. Uneven capabilities to adopt IaaS, PaaS, and SaaS could eventually leave the industry on an uneven footing in terms of resilience and security and perhaps someday be a competitive driver given the nexus of cloud services and innovation (e.g., artificial intelligence).

6.2.1 CLOUD EXPERTISE

Each aspect of running applications in the IaaS environment requires the financial institution to make unique and individual decisions at the design, implementation, and monitoring stages. Each of these stages also require decisions and input from experienced financial institution personnel in cybersecurity, business processes, and cloud architecture.

104. Fugue Inc, The State of Cloud Security 2020 Report: Understanding Misconfiguration Risk, by Drew Wright (May 2020).
105. Department of Justice, U.S. Attorney's Office, Western District of Washington, *Former Seattle tech worker convicted of wire fraud and computer intrusions* (June 2022) https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-convicted-wire-fraud-and-computer-intrusions.
106. Atlantic Council, *Broken trust: Lessons from Sunburst*, By Herr et al., (Mar. 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst.

Financial institutions noted challenges in recruiting talent to manage cloud migration and risk management. In addition to an overall skills shortage, stakeholders have indicated that financial services IT skills are not readily transferrable to the cloud environment. All of the financial institutions Treasury interviewed noted that they had to reskill or hire new talent to manage the cloud environment. Several financial institutions noted they are making a deliberate effort to upskill not only technical staff but also their business line staff to ensure that cloud computing fundamentals are at the core of their technology modernization journey. Financial institutions have increased difficulties in retention because cloud expertise is more in demand and more transferable than traditional financial services IT expertise.

These issues are particularly acute for small and medium-sized institutions wanting to take advantage of IaaS benefits for cloud storage but lacking expertise. In some cases, these institutions may overly rely on consultants or intermediary companies to access public cloud offerings. Suppose the consultant or intermediary provider has made an error that results in a vulnerability in the deployment of an application running in an IaaS environment. In that case, financial institutions may not be able to detect it until too late.

6.2.2 GAPS IN TOOLS

Some external stakeholders stated that another root cause of misconfiguration is that the cloud environment is not always built with user design in mind. IaaS offerings look significantly different from provider to provider, and may even have some differences between regions served by the same provider. Additionally, while supporting flexibility and customization for the client, the rapid pace of innovation associated with service offerings can be challenging for financial institutions to keep up with. Even larger, more resourced financial institutions reported backlogs in their ability to validate new updates continually. Occasionally, incidents occur because of a new incompatibility introduced by an update.

For example, to use cloud services, a financial institution must establish and manage various communication channels between the CSP and the financial institution's on-premises IT systems. These communication channels align data between the cloud and the on-premises IT systems, allow clients to access the services provided at the CSP, such as computing and data storage, and provide the financial institution with access to an interface for managing the cloud services. Options include APIs, encrypted communications over the public internet, and private networks. If not secured, malicious actors can exploit these communication channels. Stakeholders and other sources identified the following challenges associated with securing communications to the cloud services: (i) an increasing number of cloud service offerings by providers and related APIs increasing the complexity of identifying, securing, and managing such connections; and (ii) understanding and effectively overseeing a CSP's approach to the security of those communication connections under control of the CSP. There are some mitigating controls

for these challenges through encryption or private data connections, but the fundamental problem is identifying when and how to deploy these mitigating controls. This approach will, in turn, depend on how financial institutions understand the necessity of these controls and the cost associated with them.

Financial institutions and CSPs have taken steps to address both aspects of this challenge. Industry and financial authority toolkits and best practices for financial institutions continue to evolve. For example, the Cyber Risk Institute's cloud profile provides financial institutions with a framework to evaluate cybersecurity risk with cloud services. Some financial sector stakeholders suggested that the FBIIC and FSSCC could play a role in convening key financial institutions to discuss best practices as they evolve. While misconfiguration is generally seen as a user issue, CSPs seem to recognize the challenges of trying to market the security benefits of cloud services if clients experience prominent data breaches. CSPs are increasing educational events and deploying more automated tools and dashboards to help users identify key misconfigurations. Some financial institutions suggested that CSPs should attempt to provide some guidance on appropriate or baseline security and resilience configurations. Others noted that the complexity associated with IaaS is magnified when using multiple CSPs, which can increase risk.

6.3 EXPOSURE TO POTENTIAL OPERATIONAL INCIDENTS, INCLUDING FROM INCIDENTS ORIGINATING AT A CSP

As discussed in Section 3, many financial institutions report that cloud services can offer a number of opportunities to increase the resilience of a financial institution's technology architecture. However, many of these options are often self-contained within the service offerings of a single CSP. When financial institutions consider trade-offs accompanying an increased reliance on a third-party service, they usually consider (i) the importance of a business function and then the importance of a service to that business function; (ii) the expected resilience of the service; and (iii) substitutability of the service, including whether they could replace the service in the short-term.

In interviews, some financial institutions conveyed that there were gaps in their ability to assess the resilience of their configuration of a cloud service. Contributing factors included (i) difficulty in understanding their responsibilities or effectiveness of their choices for configuring the cloud services for the appropriate level of resilience; (ii) the lack of specific recovery time objectives in some contracts with CSPs; (iii) the lack of specific incident notification and response procedures in some contracts with CSPs; and (iv) the lack of detail in cloud service documentation regarding resilience dependencies, such as a CSP's reliance on other suppliers of IT services or internal CSP resources (such as other CSP operating regions).

Financial institutions and other sources indicated that some CSPs may provide limited cooperation in direct testing of a financial institution's business resumption and recovery capabilities. Some financial institutions noted a lack of clarity on how CSPs test and stress

their business continuity capabilities. One financial institution expressed concern that it is challenging for them to validate or test whether the CSP could support the financial institution's contracted resilience option in a second, separate CSP region if there was a severe disruption in the primary CSP region impacting many CSP clients.

Cloud services, like any service, have the potential for technical vulnerabilities that can negatively affect the confidentiality, integrity, or availability of cloud services for all customers. Technical vulnerabilities in underlying cloud service infrastructure are similar to a vendor disclosing a vulnerability in commonly used software that may impact all the users of that software. However, when the CSP is responsible for and controls the vulnerable systems in the affected service, cloud service users are entirely dependent on the CSP for the timing and effectiveness of the vulnerability remediation. For example, the extensive Log4j vulnerabilities announced in December 2021 revealed that cloud users across multiple providers had been susceptible to a previously unknown vulnerability and were left exposed from the time of the vulnerability's disclosure until the implementation of fixes by the cloud providers.[107] Compounding this problem, cloud users were also responsible for remediating the same vulnerabilities in the systems running on cloud services but under their control.

In effect, widespread vulnerabilities may require action by both the service provider and the service user. From the service provider perspective, vulnerability mitigation is often an all-or-nothing scenario, meaning the service provider has either fixed the issue for all its users or for none. Cloud users, on the other hand, may implement fixes on their side at their discretion. In the Log4j example, major cloud service providers provided transparent updates to their customers about the remediation status of vulnerabilities on their side of the shared responsibility model and encouraged their customers to remediate the systems under the cloud user's control.[108]

Software failures can cause cloud service outages. For example, in December 2021, several AWS services in an entire AWS region suffered a service disruption. The incident was caused by an unexpected internal system behavior that ultimately congested the network leading to further cascading issues that led an outage for those services.[109] The incident lasted several hours while AWS engineers identified and then resolved the problems and made changes to prevent the same type of issue from occurring in the future.

Many industry stakeholders noted the risk that a software failure could affect a key service that underpins other cloud applications, potentially affecting multiple regions. In March 2021, an update to an authentication system caused a nearly global outage of Microsoft's

107. Palo Alto Networks, Log4j - Initial Access to the Cloud, by Arazai et al. (Mar. 2022) https://www.paloaltonetworks.com/blog/security-operations/log4j-initial-access-to-the-cloud/.
108. AWS, *Apache Log4j2 Issue (CVE-2021-44228)* (Dec. 2021), https://aws.amazon.com/security/security-bulletins/AWS-2021-005/; GCP, *Apache Log4j 2 Vulnerability* (Last updated Mar. 2022), https://cloud.google.com/log4j2-security-advisory; Microsoft, *Updated: Azure DevOps (and Azure DevOps Server) and the log4j vulnerability,* by Gloridel Morales, (Dec. 2021), https://devblogs.microsoft.com/devops/azure-devops-and-azure-devops-server-and-the-log4j-vulnerability/.
109. AWS, *Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region* (Dec. 2021), https://aws.amazon.com/message/12721/.

cloud services.[110] Microsoft confirmed that any service that relied on its identity and access management (IAM) Azure Active Directory might have been affected. Services like Microsoft 365, as well as Microsoft's other cloud service offerings, were affected by this issue because IAM is a key underlying service that supports nearly all of Microsoft's cloud service offerings. The failure of this underpinning software had widespread effects for the operational resiliency of reliant services.

Although the SolarWinds incident in December 2020 yielded no known operational resilience impact to cloud service customers, the incident revealed weaknesses in IAM and privileged access management (PAM) that the threat actor used across multiple cloud service users in the cloud environment.[111] Exploitation like this could enable other malicious activity that could potentially affect the operational resilience of the users of those services, reinforcing the importance of security and resilience of lynchpin services like IAM.[112]

Another software failure involving a lynchpin service affected Akamai in July 2021. In this case, Akamai's Edge DNS Service suffered an outage following a software update that introduced a bug in the domain name system service.[113] This service outage left many websites, including those of major financial institutions and other major companies around the world, unreachable. Further, this critical service outage impacted access to internet resources to such an extent that other CSP services were also negatively affected until Akamai rolled back the update.[114]

Because using cloud services can require internet connectivity to cloud data centers, physical events can potentially disrupt services. For example, a power outage in December 2021 in AWS's us-east-1 region caused an outage at one of its data centers.[115] In addition to affecting a variety of services, the single sign-on service within the area also started to see increased failure rates, suggesting that services not directly affected by an outage may still suffer ill effects from diminished capability within a region. AWS recommended customers fail away from the affected zone even if the outage did not directly impact them.

Another physical event involving a cooling system failure at a data center impacted multiple GCP services in July 2022 in the europe-west2-a zone.[116] In this case, however, the outage affected services outside of the affected region because early mitigation attempts inadvertently modified traffic routing to avoid three zones rather than just the one with the

110. Caroline Donnelly, *Microsoft cloud users hit by global outage linked to Azure Active Directory issue*, Computerweekly.com (Mar. 2021), https://www.computerweekly.com/news/252497921/Microsoft-cloud-users-hit-by-global-outage-linked-to-Azure-Active-Directory-issue.
111. Louis Columbus, *SolarWinds breach exposes hybrid multicloud security weaknesses*, VentureBeat (May 2021), https://venturebeat.com/2021/05/15/solarwinds-breach-exposes-hybrid-multi-cloud-security-weaknesses/.
112. Atlantic Council, *Broken Trust.*
113. Mehta et al., *Websites back up after brief global outage linked to Akamai*, Reuters (July 2021) https://www.reuters.com/technology/websites-airlines-banks-tech-companies-down-widespread-outage-2021-07-22/.
114. Ibid.
115. Frederic Lardinois, *AWS just can't catch a break*, TechCrunch (Dec. 2021), https://techcrunch.com/2021/12/22/aws-just-cant-catch-a-break/.
116. GCP, *Multiple Cloud products experiencing elevated error rates,* (July 2022), https://status.cloud.google.com/incidents/fmEL9i2fArADKawkZAa2.

data center cooling system failure. Additionally, with the regional traffic routing change, GCP's regional storage services that replicate customer data across multiple regions became inaccessible. GCP recommended workarounds for some of the impacted services, including failing over to other zones when possible.

These incidents stress the importance of financial institutions understanding the risk of any cloud service, as well as the efforts that CSPs are taking to remediate and lower the risk of technical vulnerabilities in the future. While financial institutions have limited control over risks from system-wide technical vulnerabilities, they choose what workloads to deploy on public cloud services and with which vendors. Depending on the service, financial institutions can make a number of design choices that affect the resilience of the service, including deploying on multiple geographic regions. Interviews with smaller institutions revealed that they would be challenged in achieving the scale to take advantage of some of these options. First, these institutions may use managed service providers or other intermediaries because the inherent cost and complexity of running IaaS and PaaS is beyond their capabilities. These intermediary providers may not offer the same options in terms of redundancy on different data centers or with a separate geographic region. Second, even if operating directly in a major CSP environment, these enhanced resilience options may be cost-prohibitive for smaller financial institutions.

While many financial institutions can increase resilience by operating in multiple regions of the same CSP, few experts believe that complex use cases can be developed to support seamless failover from one CSP environment to a different CSP environment. Reasons include the inherent differences among service offerings, the associated complexity of designing across multiple cloud environments, and the need to hire multiple staff familiar with various environments. While complete portability appears to be the idealized solution to solve dependencies, it is not currently, nor is it likely to become, technically practical for many complex services. One key impediment is a lack of interoperability in identity and access management services across the major cloud providers and third-party solutions. Even if it became more practical, instantaneous substitutability might come with challenges that may make it inadvisable for many financial institutions and use cases (e.g., due to greater risks and costs required to design and secure multiple environments).

Some financial institutions may rely on multiple providers for different services and emphasize portability over the medium or long-term, but this is generally not a strategy that can address operational continuity in the short-term. Financial institutions also plan for how to exit a cloud relationship. But at a practical level, most exit plans are oriented around a time frame of months to years, given the difficulty in transitioning either back to on-premises or another provider.

In contrast to financial institutions that used multiple CSPs for different use cases, some financial institutions preferred relying on a single CSP. These institutions argued that deploying on multiple cloud environments had significant fixed costs in terms of developers, engineers, and risk specialists who are familiar with or need to be trained on

the specific nuances of each vendor's offerings. Even if these teams were in place (which would be difficult, given the shortage of talent), they assessed that the benefits would not outweigh the risks, including decreased capabilities to monitor the whole cloud environment.

6.4 POTENTIAL IMPACT OF MARKET CONCENTRATION IN CLOUD SERVICE OFFERINGS ON THE SECTOR'S RESILIENCE

As discussed elsewhere in this report, there is evidence that the financial sector's adoption of cloud services is notable and growing, particularly with the three major CSPs: AWS, GCP, and Microsoft Azure. A large system failure or data breach at one of these CSPs could impact multiple financial institutions or U.S. consumers, though there are open questions about the extent of that impact. Such an incident could take several forms, including:

- A service interruption or degradation in performance to a single systemic financial institution or financial market infrastructure that depends on cloud services for functions critical to the financial sector;
- A service interruption or degradation in performance to a significant segment of smaller financial institutions that depend on cloud services for material business lines; or
- An interruption or degradation to cloud services that a significant number of financial institutions rely on for critical functions or material business lines. Additionally, a widespread incident could affect other service providers used by financial institutions that also rely on cloud services.

These incidents could have a range of causes. For example, a software vulnerability discovered in a widely deployed cloud service could affect several financial institutions that have adopted the service. There also could be a scenario where existing CSP clients exhaust the available computing resources in a particular region, resulting in degraded performance for all other institutions in contention with the same resources for cloud services.

At the same time, the mere presence of large CSPs is not necessarily an issue for the financial sector's operational resilience.[117] Evaluating the operational risks that could arise from concentration in cloud services depends on how firms use and design these services. The scale that some CSPs offer have potential benefits, for example in faster patching against zero-day exploits.

A lack of aggregated data to assess concentration is a key impediment to understanding the potential impact of a severe, but plausible operational incident at a CSP on the financial sector. The following issues are significant barriers to such a mapping exercise: (i)

117. As noted previously, this report focuses on assessing operational risks associated with cloud services. Broader issues with cloud services, such as those associated with competition and market concentration more generally, are outside of the scope of this report. Some potential implications between market concentration and its effect on bargaining power are explored under the related issue of contracting for cloud services.

the lack of common definitions or identification approaches for critical or material cloud services used by financial institutions, (ii) the lack of a common and reliable method to measure concentration, (iii) different data collection authorities and mandates across FBIIC-member agencies.

The lack of common definitions focusing on the criticality of cloud services or third-party services more generally is a significant hurdle. The full range of services that financial institutions consume is not necessarily relevant to assessing the resilience of core business operations or critical functions provided by the financial sector. Common definitions recognized by financial institutions and regulators would aide in mapping critical dependencies more consistently and precisely. Meaningfully aggregating this data may require specificity in how financial institutions measure and set thresholds for (i) the importance of the business line or activity that is supported by a cloud service, and (ii) the importance of the cloud service to that business line or function.

Other jurisdictions, like the UK and EU, have experimented with registries for outsourcing and other third-party relationships in recent years but have yet to devise a model to avoid capturing too many, or too few, service relationships. Still, it may be helpful to generate an initial starting point for identifying concentration even if such inventories would have limited sensitivity to the criticality of a particular service.

While there are data gaps in terms of how critical specific cloud services may be to the financial sector as a whole, FBIIC-member agencies have a range of tools derived from applicable statutory authorities to evaluate the risk of cloud services with respect to the institutions they supervise. No single agency can view the entire financial sector, however. Agencies can collaborate through many formal and informal channels, but Treasury assesses that there are opportunities to expand these efforts. Expanding interagency coordination and closing existing data gaps will be more important as critical financial sector applications are moved to the public cloud.

Treasury also sees opportunities to enhance public and private sector coordination on cloud services. For example, financial sector incident response plans, including at the FBIIC and at the G7, typically contemplate incident coordination among financial authorities and the financial sector but have not considered direct involvement by a CSP. Given the increasing trend of cloud adoption in the industry, strengthening direct coordination and communication channels may support resiliency efforts in the event of a major cloud-related incident. More specifically, several financial institutions stressed the need for CSPs to participate in sector-specific exercises to help regulators and financial institutions better understand the impact of an operational incident to cloud services.

2022 TABLETOP EXERCISE

In April 2022, Treasury conducted a tabletop exercise examining a hypothetical service interruption at a major IaaS provider that featured participation from large financial institutions, CSPs, law enforcement agencies, financial services sector information sharing organizations, financial regulatory agencies, and other relevant U.S. government departments and agencies. The exercise aimed to:

- Discuss information sharing practices between large financial institutions, CSPs, and government entities (including regulators) during an incident affecting cloud services.
- Identify resilience and recovery options and socialize resources available to CSPs and large financial institutions during the management of a cloud service disruption.
- Improve understanding of how a cloud outage may cause operational impacts for the financial sector.

The discussion highlighted the importance of maintaining existing client-vendor communication channels. Participants also agreed on the need for follow-on work to facilitate a better understanding of potential operational consequences to the financial sector stemming from an impact to an IaaS provider.

6.5 DYNAMICS IN CONTRACT NEGOTIATION GIVEN MARKET CONCENTRATION

Stakeholders noted that contract negotiations between CSPs and financial institutions were particularly challenging. Because cloud services are offered across multiple jurisdictions and to many clients, CSPs have strong incentives not to negotiate individually where possible.

Among IaaS offerings, while financial institutions and other firms report there is still competition among the three major U.S. CSPs, even the largest financial institutions reported difficulties in negotiating contracts. One financial institution stated that when negotiating with a CSP as one of the financial sector's early adopters, the offered contract would have provided the CSP with unilateral termination rights without notice, which it could not accept. Eventually, the financial institution was able to negotiate a notice period for termination.

Negotiations are even more inflexible for SaaS offerings and smaller financial institutions. One smaller financial institution reported difficulty securing its preferred backup configuration because they did not have the scale for the SaaS provider to offer backups as part of its normal configuration. Another financial institution noted the importance of addressing how CSPs will handle encryption keys to allow access to data should they exit from the service arrangement with the provider. Some financial institutions stated that they believed obtaining audit rights within a cloud service contract was more difficult

for U.S. financial institutions. They pointed to foreign regulatory guidance as making a difference, like the European Banking Authority's outsourcing guidelines, which requires financial institutions to obtain audit rights.[118]

Financial institutions reported that some of these contractual challenges have been resolved as CSPs gained more experience working with financial institutions and became more familiar with the rationale for the regulatory expectations underpinning requests from the financial sector. Interviews with larger financial institutions indicated that, in some cases, they have more favorable treatment than smaller financial institutions when it came to certain issues like audit rights and access to information.

6.6 INTERNATIONAL LANDSCAPE AND REGULATORY FRAGMENTATION

Financial institutions, CSPs, and other external stakeholders raised the challenges associated with the increasingly complex and diverse international financial regulatory landscape for cloud services. Several stakeholders noted foreign regulators had a higher level of scrutiny over the use of cloud services, which they attributed to several factors, including unfamiliarity by some regulators, historical lack of cooperation by CSPs in the early days of adoption, and concerns regarding the privacy of data. Some global financial institutions reported that because of differences in regulatory and supervisory approaches across the globe, consistent adoption of cloud in different jurisdictions is practically impossible. This impediment potentially increases operational risks associated with the cloud because of the complexity of either managing multiple small cloud deployments or trying to manage two different cloud strategies between their U.S. technology footprint and foreign technology footprint.

Requirements for data localization pose another challenge. Such requirements can lead to a fragmentation of the technology architecture for internationally active financial institutions, which can decrease their cyber and operational resilience. To the extent that data privacy concerns drive data localization, greater cooperation among like-minded authorities (such as through the Trans-Atlantic Data Privacy Framework)[119] should ease these pressures.

CSPs and financial sector stakeholders noted the lack of common definitions, particularly concerning what may constitute "critical" or "material" services under different regulatory frameworks. These inconsistencies can cause confusion regarding complying with various regulatory expectations relevant for cloud services, for example, understanding which policies and expectations do and do not apply to different service offerings and configurations. Some jurisdictions have also implemented specific requirements or

118. EBA, *EBA Guidelines on outsourcing arrangements* (Feb 2019), https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.
119. The White House, *United States and European Commission Announce Trans-Atlantic Data Privacy Framework* (Mar. 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

guidelines for cloud or third-party providers that may be technically impractical, like mandates to use local cloud providers for primary and backup applications.

Several stakeholders Treasury interviewed noted that new foreign regulatory approaches in the EU and the UK for critical third-party providers to the financial sector could have a major effect on how CSPs engage with the financial institutions. These frameworks could increase the overall resilience of cloud services, providing positive spillovers to the U.S. financial system. But such frameworks may be challenging for CSPs to accommodate if requirements are conflicting or pose potential security risks. The impetus for these regulatory reforms includes increasing cloud adoption by larger foreign financial institutions in these jurisdictions. As such, the resilience and security of the services offered by U.S. CSPs are not just relevant to the resilience of U.S. financial system but may also be relevant to the global financial system. Treasury has led U.S. engagement on both frameworks, including through ongoing bilateral regulatory dialogues with the EU and UK, and will consider how to engage on a technical and operational level moving forward. Potential avenues include bilateral engagement, as well as the G7 CEG and the Treasury-FRB Critical Provider Dialogue.

Some stakeholders noted that cloud services lack a mature regulatory framework in emerging markets. Like small and medium-sized institutions in the U.S., financial institutions in these jurisdictions may be considering or adopting cloud services but outside a mature regulatory framework for operational risk. As cloud adoption in these jurisdictions increases, regulators in these jurisdictions may also consider expanding their regulatory perimeter over CSPs. This reality could amplify the risks of regulatory fragmentation and ultimately impact the consistency, security, and resilience of services that CSPs offer. The lack of a mature framework makes the regulatory environment for financial institutions unpredictable in certain jurisdictions. Some stakeholders conveyed that the U.S. and other advanced economies might reduce the risks of regulatory fragmentation by sharing best practices and providing more transparency over their regulatory activities.

Additionally, international coordination among financial regulators on identifying vulnerabilities or joint exercises involving CSPs – i.e., pre-incident oversight and preparation – is still being developed. It is possible that the financial authorities in one jurisdiction may identify a vulnerability that is relevant to other jurisdictions but are not committed to sharing their findings. Foreign financial authorities may also need to establish clearer protocols for how supervisory and regulatory activities involving CSPs are shared and coordinated with authorities for economy-wide cybersecurity or technology procurement.

Stakeholder concerns over regulatory fragmentation are not only limited to the international landscape. Some small banks stated that regulatory requirements applicable to banks were more rigorous than those applicable to non-bank competitors, suggesting that there may not be a level playing field for sensitive financial data.

7. Areas for Further Consideration and Next Steps

Treasury recognizes that the U.S. financial services sector employs a wide range of cloud adoption models and that it is highly likely that cloud adoption will continue to accelerate. This adoption is driven in part by cloud services facilitation of remote working arrangements and enhanced data analytics, as well as the potential for financial institutions to use the cloud environment to connect with third-party providers and clients more efficiently and securely. For some entities, cloud services represent a significant evolution in the back-end processing for financial services transactions. However, these benefits can only be harnessed if the selected services are adequately designed and managed for the appropriate level of security and resilience.

Ultimately, cloud adoption is a decision that should be and is made by each U.S. financial institution based on its own risk tolerance, risk management framework, and business needs and objectives. Treasury neither endorses nor discourages cloud service adoption by the sector. But given the growing importance of cloud services to the sector, Treasury assesses that it is appropriate to take actions to support a resilient environment for cloud adoption.

NEXT STEPS

Treasury plans to continue engagement with U.S. financial regulators, the private sector, and international partners to address the challenges identified in this report. Such steps will include:

- Establish an interagency Cloud Services Steering Group to coordinate on issues raised in this report.
- Follow-up tabletop exercises involving CSPs and the financial sector.
- Further domestic collaboration on areas implicated in this report, including developing options or approaches with respect to the following:
    - Interagency coordination and collaboration regarding potential risks posed by cloud services, including additional information-sharing opportunities;
    - Common definitions and terms across the sector, such as for “critical” services;
    - Sector-wide measurement of the concentration of critical uses of cloud services and similar third-party services;
    - Incident response involving cloud services, such as updating processes to expand communication channels between U.S. financial regulators, CSPs, and financial institutions; and
    - Financial institution risk management practices for cloud services (e.g., discussing with U.S. financial regulators where regulatory guidance could be enhanced).

- Continued support for the development of international standards, principles, and recommendations, as appropriate, including by the G7, Financial Stability Board, and the international financial standard-setting bodies.

Improved international coordination with key partners, building on existing bilateral relationships and dialogues, as well as further developing multilateral relationships, including through the new Treasury-FRB Critical Provider Dialogue.

Treasury also will consider other collaborative projects regarding cloud services. Such work could include:

- Fostering industry consensus around effective security controls, risk management practices, and contractual requirements, particularly for the benefit of small and medium-sized financial institutions, and;
- Strengthening avenues for communication with the private sector, such as around threat intelligence sharing.

PAGE LEFT INTENTIONALLY BLANK

Annex A: The Department of Treasury's Cloud Strategy

1. STRATEGIC TECHNOLOGY LANDSCAPE

To address unique mission priorities, Treasury and many of its Bureaus have adopted cloud using various service delivery models, often through duplicative contract actions and engineering efforts. This approach, while offering faster deployments, does not capitalize on opportunities for operational efficiencies, standardized security, and cost reduction through service deduplication and consolidated procurement.

Treasury's Office of the Chief Information Officer (OCIO) has established three strategic objectives in its adoption of the cloud:

- Support the Treasury mission by enabling infrastructure efficiency, scalability, and elasticity;
- Reduce inefficiencies across the Department by developing enterprise shared services that Offices and Bureaus can readily consume; and
- Secure Treasury systems using a zero trust security model.

Treasury will use these objectives to develop a detailed strategic implementation approach for managing its data, infrastructure, and application landscape. While Treasury intends to use multiple cloud providers for the delivery of its government and citizen-facing services, there will likely be some residual on-premises infrastructure that must be maintained for mission-specific purposes. Treasury will use its Cloud Program Office to provide and promote effective governance and technology management for cloud services. Through policies, solutions architecture, and knowledge sharing, the Cloud Program Office will be a mechanism for the entire Department to achieve its enterprise cloud infrastructure goals.

2. STRATEGIC OBJECTIVES

Treasury is transforming its infrastructure to accommodate modern demands and better enable mission delivery by improving the reliability, security, and resiliency of technology services. Today, Treasury has a hybrid multi-cloud infrastructure that serves as a general-purpose platform for Department-wide use cases (e.g., human resources management) and a fit-for-purpose cloud specifically for tailored use cases. Treasury has managed IaaS, PaaS, and SaaS service delivery models.

While adopting the existing cloud environment has been consistent, Treasury will be developing a new enterprise cloud offering that will accelerate adoption and enable the Department and its Bureaus to gain efficiencies in access, scale, cost, contracting, and security. By combining purchasing power and reducing duplicative capabilities, Treasury can achieve greater cost control through economies of scale at the enterprise level that exceeds those that the Bureaus can reach independently. Treasury can use

these savings to capitalize on future investments and allow Treasury to obtain higher levels of service. This enterprise infrastructure cloud strategy enables centralized infrastructure management, which lessens the operational burden for Bureaus while providing Treasury leadership an overall view of utilization, costs, and security posture. During Fiscal Year 2023, a contract will be awarded for "Treasury Cloud" - a fully managed multi-cloud environment. The decision to pursue a multi-cloud contract is largely based on the diversity of our mission activities. Treasury bureaus are engaged in broad-ranging technical and operational activities, from the manufacture of currency in factory environments (e.g., the Bureau of Engraving and Printing and the U.S. Mint) to the administration of taxes through physical and digital intake channels. While there is a high degree of parity in the foundational capabilities of each CSP, there are nuanced differences that make it preferable for Treasury to rely on different CSPs for certain use cases.

2.1 SENABLE INFRASTRUCTURE EFFICIENCY, SCALABILITY, AND ELASTICITY

By implementing a hybrid infrastructure solution that links on-premises and cloud-based compute, storage, and network capabilities, Treasury has accomplished a highly reliable, efficient, and agile infrastructure. This infrastructure brings cost-efficient scalability and elasticity to long-term and episodic requirements, which limits capital outlays and avoids the cumbersome and lengthy acquisition and implementation cycle of traditional IT infrastructure.

The adoption of cloud infrastructure technologies in the Treasury enterprise has alleviated challenges in managing computing, storage, and networking. It provides flexibility, empowering Treasury to redirect scarce resources to mission-critical efforts instead of owning and managing commodity infrastructure technologies. Many of our data centers are in facilities that have not been appropriately modernized or do not reside within purpose-built structures (e.g., inside a federal office building). Some reside in geographical regions where technical talent is in shorter supply. By consolidating our data center footprint to commercial facilities and transferring workloads to the cloud, we will be less hindered by insufficient computing, storage, and network capacity and the potential for catastrophic failures introduced by the physical plant.

By implementing an on-demand scalable infrastructure, Treasury has started gaining significant efficiencies in the execution of its mission, as the shared cloud infrastructure enables teams to deploy and scale rapidly. Additionally, enterprise cloud solutions will allow Treasury to further consolidate much of its legacy on-premises assets, increasing compliance with OMB data center consolidation initiatives.

2.2 REFORM IT AT THE DEPARTMENT BY EMBRACING CLOUD

To meet modern computing and storage practices, Treasury has adopted a consumption model by gradually trading capital expenses for operating expenses to optimize costs across its technology portfolio and allow for adaptation to changing priorities, budgetary conditions, and industry developments. The cloud environment provides financial

flexibility through the provisioning and de-provisioning of resources automatically to provide optimum asset management when compared to traditional IT infrastructure, which is constantly in operation even when utilization is low or nonexistent.

This efficiency will gradually improve the Government's budgeting, billing, and payment practices by providing detailed resource usage reports for all mission owners while creating transparency to drive further efficiencies. The Treasury's Cloud Program Office is integrating with Treasury's Technology Business Management (TBM) processes for reporting to better track financials and cloud resources.

2.3 IMPLEMENT MODERN CYBERSECURITY FRAMEWORKS TO SECURE TREASURY SYSTEMS

Treasury's cloud platform has begun to shift its security focus from perimeter defense to a zero trust model of securing data, users, and services. We will accomplish this shift through strong authentication for users and machines, encryption of data both at rest and in transit, and cloud-based policy enforcement points for all traffic. The Treasury cloud infrastructure environments leverage native and third-party cloud services to encrypt communications, endpoints, and storage by default. Treasury plans to further implement zero trust principles, leveraging concepts such as TIC 3.0 for systems and applications, following the NIST, CISA and OMB guidance, building on the zero trust architecture offered by its current cloud platform.

3. STRATEGIC APPROACHES AND GUIDING PRINCIPLES

Treasury utilizes a multi-cloud approach, which provides an environment of private, public, and hybrid clouds. To achieve the objectives outlined previously, the Treasury Cloud Strategy is based on a set of principles, guiding the efficient utilization of cloud resources: Cloud Infrastructure Sharing; Cloud Infrastructure Best Practices; Cloud Infrastructure Workforce; and Cloud Infrastructure Strategic Sourcing.

3.1 CLOUD INFRASTRUCTURE SHARING

To achieve the strategic principles outlined, the Treasury OCIO has built a cloud infrastructure specifically to be used for shared services called Workplace Community Cloud (WC2). It currently resides on AWS and is expanding to Microsoft Azure and will likely expand to other CSPs in the future. The WC2 program provides migration and hosting of Department and Bureau applications and data, supporting plans for reducing the existence of data centers. As previously mentioned, the program is assessing WC2 platform upgrades to implement TIC 3.0 policy enforcement points as part of our overall zero trust architecture.

3.2 CLOUD INFRASTRUCTURE BEST PRACTICES

To support an enterprise cloud infrastructure strategy, Treasury leverages best practices across the Treasury Department, Federal Government colleagues and partners, NIST, and

the commercial industry. Treasury's Cloud Program Office has been leveraging commercial cloud offerings to benefit from the natural competitive processes between CSPs that force them to evolve and mature their products quickly. Treasury is positioning itself to get the best value in today's market of cloud computing capabilities to support business requirements and to grow its capabilities as the industry evolves.

3.3 CLOUD INFRASTRUCTURE STRATEGIC SOURCING

To facilitate its cloud strategy, Treasury has developed governance approaches for standardization and centralization, in line with the Department's IT shared services approach, that provides secure, efficient, and cost-effective business innovation. The acquisition and procurement cycles for IT and cloud infrastructure services are lengthy and occasionally negate many of the just-in-time benefits associated with cloud services. As such, Treasury has implemented a shared service cloud infrastructure model to capture Treasury-wide efficiencies in access, contracting, and security.

This enterprise-wide acquisition strategy enables Treasury to leverage long contract lifecycles with the necessary scope to provide customers the flexibility in cloud usage. This will also take advantage of the economies of scale at the Department level when buying cloud products and services and is in alignment with the Federal Strategic Sourcing Initiative and the larger Federal Information Technology Acquisition Reform Act mandate intended to streamline acquisitions, foster the sharing of best practices, and further opportunities to increase cost savings and value. Bureaus will have the chance to achieve zero trust and TIC 3.0 alignment using Treasury Cloud.

3.4 FULL EMBRACE OF THE API ECOSYSTEM

To facilitate the adoption of enterprise cloud, our consumers expect our services to be predictable, reliable, and consumable. In the current technological context, consumption is most appealing when there are defined inputs, defined outputs, and aggressive SLAs. Treasury has gravitated toward an API-driven ecosystem with standardized formats for data interchange of flat files. Common capabilities such as key management, secrets management, or identity and access management would be catalogued such that they can be easily expressed in code. Conceptually the idea is to transition the focus on stacking capabilities to drive business outcomes, with fewer resources put toward the supporting infrastructure.

Annex B: External Stakeholders Interviewed

Treasury and certain FBIIC-member agencies met with a broad array of organizations and individual companies to gain insights from practitioners on cloud adoption in the financial services industry. This included roundtable discussions with representatives of financial sector associations, cloud services providers, and research-focused think tanks. Treasury also conducted talks with individual stakeholders.

This outreach was organized under an open discussion without attribution focused on the current and future state of cloud adoption, viewpoints on the unique risks related to cloud adoption and third-party risk management processes.

PARTICIPATING EXTERNAL ORGANIZATIONS

American Bankers Association
AIG
Amazon Web Services
Atlantic Council
Bank Policy Institute
Barclays
Bank of New York Mellon
Bank of America
Capital City Bank Group
Capital One
Carnegie Endowment
Citigroup
CLS-Bank
CME Group
Commonwealth Credit Union
Center for Strategic and International Studies
Cyber Risk Institute
Depository Trust & Clearing Corporation
Deutsche Bank
Fannie Mae
Financial Services Sector Coordinating Council
Financial Industry Regulatory Authority
Fiserv
Goldman Sachs
IBM Cloud
Intercontinental Exchange
International Monetary Fund
Independent Community Bankers of America
Institute of International Finance
Jack Henry
JP Morgan Chase
KeyBank
Kyndryl
Lewis & Clark Bancorp
Mastercard
Microsoft
Morgan Stanley
First United Corporation
Options Clearing Corporation
Program on International Financial Systems
Prudential Financial
Queensborough National Bank & Trust Company
Santa Cruz County Bank
SIFMA
Simmons Bank
SWIFT
TruWest Credit Union
Wells Fargo

U.S. Department of the Treasury

TREASURY.GOV