sifma

# Navigating Regulatory Challenges in Cloud Services Agreements

March 2024

Contents

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit https://www.sifma.org/.

Bortstein Legal Group, a law firm with operations in New York, London, and Toronto, is a noted leader in the areas of technology, market data, digital content, privacy, cyber-security, outsourcing, vendor contracts and corporate real estate. Bortstein Legal Group's extensive knowledge of global laws and regulations impacting financial institutions' use of technology, data and services allows Bortstein Legal Group to help its clients ensure that their activities and contracts comply with evolving global standards. For more information, visit https://www.blegalgroup.com/.[1]

This paper is subject to the Terms of Use applicable to SIFMA's website, available at https://www.sifma.org/terms-of-use/.

[1] Bortstein Legal Group's contributors to this paper include Larry Bortstein, Lou Trotta, Benjamin Ross, James Humphrey-Evans, David Cummings, Kimberly St. Sauveur, Julian Conway, and Mark Potkewitz. Additionally, Derek Manners, Dechert LLP, made significant contributions to Section 3.H. (Books and Records).

## Introduction

SIFMA, in partnership with Bortstein Legal Group, first developed this paper in 2020 and updated it in early 2024.[2] Since 2020, the use of cloud infrastructure has grown significantly,[3] and the attention of regulators to cloud — and the broader topics of operational risk and technology risk[4] — remains high.[5] In this paper, we examine the regulatory guidance in the United States, the European Union, the United Kingdom, and Canada,[6] relevant to financial institutions' relationships with providers of cloud services such as 'Software as a Service' ("**SaaS**"), 'Infrastructure as a Service' ("**IaaS**"), 'Platform as a Service' ("**PaaS**"). Providers of cloud services may deliver their services to financial institutions directly, however, they may also deliver their services indirectly, for example, as subcontractors ("**Indirect Cloud Providers**"). Some financial institutions engage vendors to provide services (other than cloud services). This class of vendors (*e.g.*, managed and professional service providers, consultants, law firms) may significantly rely on third-party cloud services provided by Cloud Providers (as defined below) in delivering their services to financial institutions ("**Managed and Professional Service Vendors**" or "**MPS Vendors**"). For the purposes of this paper, MPS Vendors as well as SaaS Vendors, IaaS Vendors and PaaS Vendors are referred to herein as "**Cloud Providers**" and their services and products as **"Cloud Services"**. Cloud Services by Indirect Cloud Providers are also referred to herein as "**Indirect Cloud Services**".

This paper reviews the experience of financial institutions in attempting to address their regulatory expectations and guidance requirements in their agreements with Cloud Providers. It considers some of the issues that Cloud

[2] This paper is not intended to be a complete inventory and does not analyze every applicable global law and regulation. Market participants should consider obtaining independent legal advice with respect to their regulatory and compliance obligations.

[3] Fortune Business Insights, Cloud Computing Market Size, Share & COVID-19 Impact Analysis, By Type (Public Cloud, Private Cloud, and Hybrid Cloud), By Service (infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), By Industry (BFSI, IT and Telecommunications, Government, Consumer Goods and Retail, Healthcare, Manufacturing, and Others), and Regional Forecast (2023-2030) (May, 2023), https://www.fortunebusinessinsights.com/cloud-computing-market-102697 (last visited February 7, 2024).

[4] *See ,e.g.,* the more general coverage of digital operational resilience for information and communication technology in the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (hereinafter "DORA") (available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj).

[5] *See, e.g.*, Letter from Bank of England, *International banks Supervision: 2024 priorities,* 5 (available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2024/artis-2024-priorities.pdf), which reminds banks of cloud risk and the new requirements for operational resilience under supervisory statement 1/21 citing Bank of England, *SS1/21 Operational resilience: Impact tolerances for important business services* (March 29, 2021) (available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss).

[6] See The Office of the Superintendent of Financial Institutions Canada (hereinafter "OSFI"), Guideline B-10: Outsourcing of Business Activities, Functions and Processes, as supplemented by OSFI's Memorandum re New Technology-Based Outsourcing Arrangements (Feb. 29, 2012) (available at: https://www.osfi-bsif.gc.ca/Eng/Docs/b10_2023.pdf), which guides outsourcing in the financial services sector by Canadian federally regulated financial institutions (e.g., financial institutions such as banks and credit unions) (hereinafter "Canadian FRFIs"). That guideline will be replaced, effective as of May 1, 2024, by a new OSFI Guideline B-10: Third-Party Risk Management (Apr. 30, 2023) (available at: https://www.osfi-bsif.gc.ca/Eng/Docs/b10_2023.pdf) that applies broadly to third-party arrangements. References to "OSFI Guideline B-10" in this paper will refer to the updated guideline. Service Agreements entered into prior to April 30, 2023, or between April 30 2023 and May 1, 2024, should adhere to the updated guidelines or be updated as soon as possible thereafter. The Canadian Investment Regulatory Organization (hereinafter "CIRO") is a self-regulatory organization that regulates investment dealers and mutual fund dealers and that issues various rules, guidances and notices, including with respect to outsourcing arrangements and cybersecurity. CIRO incorporates some of the rules and guidances of its predecessors, the Investment Industry Regulatory Organization of Canada ("IIROC") and the Mutual Fund Dealers Association of Canada ("MFDA"). In particular, see IIROC Guidance Note "Outsourcing arrangements" GN-2300-21-003 dated October 14, 2021 (hereinafter "IIROC Outsourcing Guidance"), which incorporates concepts from Canadian Securities Administrators National Instrument 31-103, Part 11 (Sep. 2009).

Providers have raised in response to financial institutions' preferred contracting approaches, including how those requirements may conflict with Cloud Providers' "shared responsibility" models and the technical or operational capabilities of their Cloud Services. In addition, this paper identifies contractual approaches that have been employed by Cloud Providers and financial institutions to accommodate the Cloud Providers' objections while addressing the financial institutions' regulatory concerns.

Cloud Providers are central to the functioning and security of the financial system.[7] Financial institutions utilize Cloud Services to respond to customer demands for digital products, increase physical and cyber security resilience, improve operational efficiency, enhance compliance and data protection, and save money. The recent wave of digitalization in the financial sector, which continues to have transformative effects on client expectations, has underscored the need for agile, resilient, and powerful computing technology to deliver financial products and services.

The use of Cloud Services does not obviate the need for financial institutions to maintain an overall vendor management governance program as required by applicable regulations and guidance. Such a program must include appropriate internal policies and procedures relating to, among other things, vendor due diligence and on-going monitoring of vendors and vendor concentration risk in order to mitigate reputational, operational, security, financial and legal/regulatory risks associated with any such use.[8]

The financial industry's rapidly growing reliance upon Cloud Providers creates an ever greater need for ensuring that activities are performed for financial institutions in a safe and sound manner that is in compliance with applicable laws and regulations.[9] Regulators today are focused on the seriousness of cybersecurity threats and the significant

[7] *See* Joint Statement, Security in a Cloud Computing Environment, Fed. Fin. Insts. Examination Council (hereinafter "FFIEC") (Apr. 30, 2020) (available at: https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf), (hereinafter "FFIEC Joint Statement") at 3: "Careful review of the contract between the financial institution and the cloud service provider along with an understanding of the potential risks is important in management's understanding of the financial institution's responsibilities for implementing appropriate controls. Management's failure to understand the division of responsibilities for assessing and implementing appropriate controls over operations may result in increased risk of operational failures or security breaches. […] Failure to implement an effective risk management process for cloud computing commensurate with the level of risk and complexity of the financial institution's operations residing in a cloud computing environment may be an unsafe or unsound practice and result in potential consumer harm by placing customer-sensitive information at risk."

[8] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017); FFIEC, Information Technology Examination Handbook, Outsourcing Technology Services Booklet (2004), (*available at* https://ithandbook.ffiec.gov/media/pqtfvxxq/ffiec_itbooklet_outsourcingtechnologyservices.pdf, (hereinafter "FFIEC Handbook") at 18-19; FFIEC, Business Continuity Management Handbook, (available at: https://ithandbook.ffiec.gov/media/2nifgh2b/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf) (hereinafter "FFIEC BCM") at § IV.A.5, "Third-Party Service Providers". OSFI Guideline B-10, *supra* note 6, at §1. FRFIs are accountable for managing the risks arising from third-party arrangements. FRFIs should have clear governance and accountability structures in place, with comprehensive risk strategies and frameworks. As such, "the FRFI should establish a [Third-Party Risk Management Framework] that sets out clear accountabilities, responsibilities, policies, and processes for identifying, managing, mitigating, monitoring and reporting on risks relating to the use of third parties"; IIROC Outsourcing Guidance, *supra* note 6, at § 2.2 and Appendix A.

[9] FFIEC Joint Statement, *supra* note 7, at 4: "Contracts between the financial institution and cloud service provider should be drafted to clearly define which party has responsibilities for configuration and management of system access rights, configuration capabilities, and deployment of services and information assets to a cloud computing environment, among other things.". OSFI Guideline B-10, *supra* note 6, at § 4, which focused on technology and cyber risk in third-party arrangements. In particular, FRFIs "should develop cloud-specific requirements to ensure that cloud adoption occurs in a planned and strategic manner. These specific requirements should optimize interoperability while remaining consistent with the FRFI's stated risk appetite. They should also augment existing FRFI controls and standards, notably in the areas of data protection, key management, and container management" and include cloud governance." In addition, FRFIs should consider cloud portability, resilience strategies and mitigation of concentration risk.

and systemic risks that they pose to information and financial systems.[10] This regulatory focus underscores the need of financial institutions to implement cybersecurity programs that match the relevant risks and keep pace with technological advances. Cloud Services that fail to meet a financial institution's expectations could adversely affect the financial institution, including its data, financial condition, or operations, as well as those of its customers. At the same time, novel and complex technologies, such as chatbots powered by large language models, proliferate in the cloud industry today and are developing rapidly, raising unprecedented and complicated regulatory obstacles. Increasing reliance upon Cloud Providers, coupled with the release and integration into day-to-day operations of powerful novel technologies, present complex challenges to financial institutions and accelerate the need for safe and sound migration to Cloud Services by financial institutions. It is more essential than ever that financial institutions and their Cloud Providers work together to prudently manage the risks posed by their relationships.

## 1. Regulatory Expectations: Risk-Based Approach

To minimize the risks associated with outsourcing by financial institutions, including with regard to Cloud Providers, financial regulators ("**Regulators**") have issued various requirements and guidance that generally include principles for a flexible, risk-based approach to third-party risk management which financial institutions should consider when developing and implementing risk management practices for all stages in the life cycle of third-party relationships.[11] In recent years, Regulators have updated and enhanced these requirements and guidance bringing regulatory expectations and risk management practices for Cloud Services into sharper focus.[12] Viewed in the context of Cloud Providers, while some nuance exists across regulations, Regulators generally allow financial institutions to take a flexible approach in managing such third-party risks, acknowledging that different relationships present varying risks and levels of risk,[13] but on some topics Regulators can be quite prescriptive, including by issuing technical standards

[10] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017). OSFI Guideline B-10, *supra* note 6, at §§ 2.3.2, 2.4.2.2, and 4; *see also* OSFI Guideline B-13: Technology and Cyber Risk Management (Jul. 31, 2022) (available at: https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management) and OSFI, Technology and Cyber Security Incident Reporting Advisory (Aug. 13, 2021) (available at: https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-security-incident-reporting).

[11] See FFIEC Guidance *supra* note 8, at IV, 3, a Contract Negotiation, pp. 45-47; see also, FFIEC Handbook, *supra* note 8. OSFI Guideline B-10, *supra* note 6, at §§ 1 and 2.

[12] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37, 920 (Jun. 9, 2023), (available at: https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management) (hereinafter "2023 Interagency Guidance"). Note that the 2023 Interagency Guidance rescinds (i) OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; (ii) OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (OCCFAQs); (iii) Federal Reserve's SR Letter 13-19/CA Letter 13-21, "Guidance on Managing Outsourcing Risk" (December 5, 2013, updated February 26, 2021); and (iv) FDIC's FIL-44-2008, "Guidance for Managing Third-Party Risk" (June 6, 2008). 2023 Interagency Guidance at 921. Regarding the OCC FAQs, concepts from most of the FAQs are expressly incorporated throughout the Guidance; concepts from other FAQs were not incorporated because they were deemed adequately covered by other agency issuances (see p. 25). The only FAQ item expressly excluded from the Guidance is OCC FAQ 4, which discussed risk management with respect to data aggregators; rather than incorporate concepts from FAQ 4, the agencies opted "to provide broad risk management guidance[.]" *Id*. at 923. *See also*; FFIEC Joint Statement, *supra* note 7; N.Y. COMP. CODES R. & REGS. tit. 23, § 500, *et seq*.; Financial Stability Board, Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities (Dec. 4, 2023) (available at: https://www.fsb.org/wp-content/uploads/P041223-1.pdf); DORA, *supra* note 4. OSFI Guideline B-10, *supra* note 6, at § 4, with respect to high-risk and critical third-party arrangements.

[13] DORA, *supra* note 4, at Article 28(b) requires that financial entities manage ICT third-party risk in accordance with the "principle of

and specific contractual requirements.[14]

Some Regulators have encouraged financial institutions to avoid overly prescriptive approaches based solely on the type of a third party.[15] For the most part, Regulators encourage financial institutions to tailor their risk management practices to the risks presented by the particular Cloud Provider relationship and activity, managing risks based on the risk profile and complexity of the activities and Cloud Provider relationship at hand. A risk-based approach to risk management processes provides financial institutions the opportunity effectively and accurately to identify and designate those Cloud Provider relationships that warrant more comprehensive and rigorous oversight. In order to be able to do this, Regulators generally agree that financial institutions must understand the structure of their overall arrangement with a particular Cloud Provider.

Financial Institutions, for example, should weigh the overall risks associated with having only a small number of IaaS Vendors. The same IaaS Vendors that provide IaaS Services directly to financial institutions often provide IaaS services indirectly as subcontractors to many other Cloud Providers. This IaaS Vendor structure and widespread reliance on IaaS Vendors constitutes a concentration risk to financial institutions. To help mitigate this risk and others posed by Cloud Providers, Regulators expect financial institutions to secure contractual obligations from Cloud Providers that support, and are consistent with, applicable regulatory expectations and requirements

proportionality" taking into account "the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level." FRFIs should "understand the risk and criticality of each third-party arrangement" when determining "the intensity with which to apply the expectations set out in" the guideline. OSFI Guideline B-10, *supra* note 6, at § A2. OSFI acknowledges that "there are certain third-party arrangements for which a customized contract may not be feasible, or for which a formal contract or agreement may not exist", in which case risk mitigation factors should be considered. OSFI Guideline B-10, *supra* note 6, § 2.3.1.1; 2023 Interagency Guidance, *supra* note 12; "In response to concerns over the risks related to outsourcing and third-party service relationships, the FSB has developed a toolkit for financial authorities and financial institutions for enhancing their third-party risk management and oversight. Recognising differences across jurisdictions and financial institutions, the FSB has developed a flexible and risk-based set of tools ("toolkit"), which financial authorities and financial institutions may consider based on their circumstances, including the legal framework and specific features of the financial services sector in their jurisdictions. At the same time, the toolkit seeks to promote comparable and interoperable approaches across jurisdictions." Financial Stability Board, Press Release, Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities (Dec. 4, 2023) (available at: https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/).

[14] *See*, *e.g.,* Final Report, (JC 2023 86), Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority (hereinafter the "European Supervisory Authorities) (Jan. 17, 2024) (available at: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf) and Final Report on, (JC 2023 84) Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554, European Supervisory Authorities (Jan. 17, 2024) (available at https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_services_supporting_critical_or_important_functions.pdf). *See also*, OSFI Guideline B-10, *supra* note 6, at Annex 2.

[15] *See, generally,* UK Financial Conduct Authority, *Outsourcing and operational resilience* (Jan. 9, 2020, last updated Dec. 7, 2023) (available at: https://www.fca.org.uk/firms/outsourcing-and-operational-resilience). Regulators comment that "the agencies do not believe it would be appropriate to prescribe alternative approaches or to broadly assume lower levels of risk based solely on the type of a third party. For example, while a third-party relationship with an affiliate may have different characteristics and risks as compared to those with non-affiliated third parties, affiliate relationships may not always present lower risks. The same is true for third parties that are subject to some form of regulation." 2023 Interagency Guidance, *supra* note 12, at 23.

and effective risk management.[16]

Arrangements for Cloud Services can be complex.[17] An effective risk approach requires a full understanding of the structure of a Cloud Services arrangement. Responsibility for the security and availability of data and services in a cloud is always shared between the Cloud Provider and its customer (*e.g.*, responsibilities for securing hardware, infrastructure, endpoints, data, configurations, settings, operating system, network controls and access rights). Ownership of security tasks and functions will differ depending on the specific cloud delivery model (*e.g.*, SaaS, PaaS or IaaS services) and how the Cloud Provider has chosen to implement it. In some delivery models, security responsibilities vary depending on the Cloud Provider or the agreement for services. This paper discusses the complexities of Cloud Provider shared responsibility models in **Section 2 (Shared Responsibility)** and raises points to consider in connection with the different delivery models offered by Cloud Providers that are set out throughout the paper.

Appropriate due diligence and ongoing monitoring by financial institutions of each of their Cloud Provider relationships (including its subcontractors) throughout the length of the relationship is a key element to an effective, risk-based approach.[18] If the facts and circumstances — including, for example, risk profile — change in the context of a Cloud Provider relationship, financial institutions are expected to adjust their risk-based approach accordingly.[19] The level and scope of a financial institution's monitoring of a particular Cloud Provider relationship with a financial institution may vary over its lifetime, but the financial institution's monitoring of its Cloud Provider is expected to remain commensurate with the levels of risk and complexity that are associated with the relationship and services.[20]

A financial institution should independently assess and determine the relevance of the suggestions and considerations discussed in this paper to any specific Cloud Provider relationship based on the unique circumstances of the relationship between the Cloud Provider and the financial institution and the particular use

[16] 2023 Interagency Guidance, *supra* note 12, at 931: "Considerations related to operational resilience include, among other things, dependency on a single provider for multiple activities." OSFI Guideline B-10, *supra* note 6, at § 2.2.3.

[17] 2023 Interagency Guidance, *supra* note 12, at 27-28.

[18] DORA, *supra* note 4, at Article 28(4) sets out due diligence steps to be carried out by the financial entity before entering a contractual arrangement on the use of ICT services; Similarly, OSFI Guideline B-10 requires the FRFI to "undertake due diligence prior to entering contracts or other forms of arrangement with a third party, and on an ongoing basis proportionate to the level of risk and criticality of the arrangement" § 2.2.2 of OSFI Guideline B-10, *supra* note 6. *See also*, IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 5 and Appendix B. 2023 Interagency Guidance, *supra* note 12, discussing "Planning" at 928-929 and "Ongoing Monitoring" at 934 *et seq*.

[19] OSFI Guideline B-10, *supra* note 6, at § 2.2.1. Regulators list several factors that a banking organization typically considers, among others, as part of ongoing monitoring, depending on the degree of risk and complexity of the third-party relationship. 2023 Interagency Guidance, *supra* note 12, at 935.

[20] 2023 Interagency Guidance, *supra* note 12, at 934. FFIEC Joint Statement, *supra* note 7, "highlights examples of risk management practices for a financial institution's safe and sound use of cloud computing services and safeguards to protect customers' sensitive information from risks that pose potential consumer harm[,]" and, among other things, sets out examples of controls unique to the architectures of cloud computing services. *Id*. at 1. "Management should refer to the appropriate FFIEC member guidance referenced in the 'Additional Resources' section of this statement for information regarding supervisory perspectives on effective information technology (IT) risk management practices. [The FFIEC Joint Statement] also contains references to other resources, including the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Department of Homeland Security (DHS), International Organization for Standardization (ISO), Center for Internet Security (CIS), and other industry organizations (e.g., Cloud Security Alliance)." *Id*.

case.[21] Regulators and financial institutions alike generally regard Cloud Providers and their Cloud Services to be of higher, or even in some instances critical, risk to financial institutions (*e.g.*, those that significantly impact the financial institution's financial condition, operation or customers, or those that cause significant risk to the financial organization, if the Cloud Provider fails to meet its obligations).[22] As such, oversight and management by a financial institution of its Cloud Provider relationships are typically more comprehensive and rigorous than many of the financial institution's other vendors, reflecting the need to allocate resources proportionally to higher risk vendor relationships.[23]

Note that failure to comply with regulatory requirements around technology governance may well be characterized as a more general failing of a financial institution's management, rather than as a compartmentalized failure of the financial institution's technology function.[24] In some jurisdictions, such as the United Kingdom, individual executives of financial institutions can be held personally accountable by Regulators for the regulatory failings of the financial institution.[25]

## 2. Shared Responsibility

A discussed above, it is important for financial institutions to understand how their arrangement with a Cloud Provider is structured so that a financial institution can assess the types and levels of risks posed by such structure and independently determine how to manage the Cloud Provider arrangement effectively.[26]

Where a Cloud Provider provides Cloud Services directly to a financial institution, the financial institution is typically responsible for selecting the features, functions, and tools required to meet their performance expectations and regulatory needs. The financial institution is responsible for fully understanding the use case and, to the extent possible, any future use cases (*e.g.*, criticality of availability, type of data) so that the financial institution — and its users — are able to use the features, functionality and tools made available by the Cloud Provider, as appropriate, for each applicable use case. By offering a cloud delivery model that compartmentalizes each party's areas of responsibility and providing a minimum level of system security and operational capacity, the Cloud Provider

[21] 2023 Interagency Guidance, *supra* note 12, at 928: "The degree to which the examples of considerations discussed in this guidance are relevant to each banking organization is based on specific facts and circumstances and these examples may not apply to all of a banking organization's third-party relationships." OSFI Guideline B-10, *supra* note 6, at § A2: "OSFI expects FRFIs to consider risk and criticality when examining third-party arrangements to determine the intensity with which to apply the expectations set out in" the guideline.

[22] FFIEC Joint Statement, *supra* note 7, at 3. *See also* OSFI Guideline B-10, *supra* note 6, at § 4: "OSFI recognizes that technology and cyber risks in third-party arrangements present elevated vulnerabilities to the FRFI. […] The FRFI should consider additional controls to manage technology and cyber risks stemming from its third-party arrangements."

[23] DORA, *supra* note 4, at Article 4; OSFI Guideline B-10, *supra* note 6, at §§ 2.1 and 2.2.

[24] *See* News release, TSB fined £48.65m for operational resilience failings, The Bank of England (Dec. 20, 2022), (available at: https://www.bankofengland.co.uk/news/2022/december/tsb-fined-for-operational-resilience-failings), discussing the UK Prudential Regulation Authority's finding that a financial institution's technology breach was also a breach of Fundamental Rules.

[25] *See* News release, PRA fines the former Chief Information Officer of TSB Bank plc for a breach of the PRA's Senior Manager Conduct Rules (Apr. 13, 2023) (available at: https://www.bankofengland.co.uk/news/2023/april/pra-fines-former-cio-of-tsb-bank-plc-for-breach-of-pra-senior-manager-conduct-rules).

[26] "An effective inventory process for the use of cloud computing environments is an essential component for secure configuration management, vulnerability management, and monitoring of controls." FFIEC Joint Statement, *supra* note 7, at 5.

effectively limits its liability for ensuring access to, and safeguarding the security of, the services in the cloud, including associated data.

Regulators generally expect financial institutions to enter into written agreements with Cloud Providers ("**Service Agreements**"), and advise financial institutions to carefully identify the appropriate level of due diligence to be performed on a particular Cloud Provider arrangement, including a careful examination of the Cloud Provider's model of service in the context of the financial institution's use case.[27] This includes a review of the applicable Service Agreement and Service Level Agreements to ensure that the financial institution is fully aware of its security responsibilities and to identify any potential gray areas that may need to be clarified.[28] If the financial institution does not fully understand its respective shared responsibilities in connection the Cloud Services, as well as any applications, data or activity associated with them, it may leave its data and the Cloud Services insecure. This can result in a financial institution unknowingly running workloads in a public cloud that are not fully protected, which would make such workloads and financial institutions vulnerable to attacks that target the operating system, data, or applications.

To mitigate risks associated with a Cloud Provider's failure to provide features, functionality and/or tools required to meet performance expectations and regulatory needs, a financial institution should consider obtaining a commitment by the Cloud Provider in their Service Agreement to provide and maintain the features, functionality and tools necessary for all use cases and should ensure that such features, functionality, and tools all work properly before deploying the services for the intended use case.[29]

Indirect Cloud Services can further complicate a financial institution's arrangement with an MPS Vendor given the use of a shared responsibility model in the provision of Cloud Services. A full understanding of the roles and coordination required between the MPS Vendor, its Indirect Cloud Provider, the financial institution, and other vendors, if any, is a necessity to effectively manage the risks posed by such arrangements. An MPS Vendor, for example, will likely need to retain privileged access to the service and hence become a third participant in the shared responsibility model. The MPS Vendor may be responsible for configuring the service securely, building applications on the cloud platform, performing effective monitoring, and ensuring business resilience. In this case,

[27] *See supra* note 8. OSFI Guideline B-10, *supra* note 6, at § 2.3.1 "OSFI expects third-party arrangements to be supported by a written contract or other agreement (e.g., service level agreement) that sets out the rights and responsibilities of each party and which has been reviewed by the FRFI's legal counsel", as well as the due diligence expectations in § 2.2. Note that at §§ 2.3.1 and 3, "OSFI recognizes that there are certain third-party arrangements for which a customized contract may not be feasible, or for which a formal contract or agreement may not exist". OSFI has listed various expectations for risk mitigation in such situations.

[28] DORA, *supra* note 4, at Article 28(5) provides that "financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards." OSFI Guideline B-10, *supra* note 6, at § 2.3.2: "Third-party agreements are expected to set out each party's responsibilities for the confidentiality, availability and integrity of records and data." *See also*, FFIEC Joint Statement, *supra* note 7, at 2.

[29] FFIEC Joint Statement, *supra* note 7, at 2: "The contractual agreement between the financial institution and the cloud service provider should define the service level expectations and control responsibilities for both the financial institution and provider. Management may determine that there is a need for controls in addition to those a cloud service provider contractually offers to maintain security consistent with the financial institution's standards."

the financial institution should consider assessing the MPS Vendor as if it were the financial institution's primary cloud service provider. Some of the financial institution's risk management goals will be achieved natively by the underlying cloud, while others will need to be addressed through considering how the MPS Vendor operates and configures the financial institution's instance of the Cloud Service.

In addition, and as discussed further in **Section 3 (Contract Terms)**, the Service Agreement should address the respective responsibilities of the parties to, among other things, facilitate effective risk management and oversight. The MPS Vendor should be contractually obligated in its Service Agreement with the financial institution, for example, to provide and maintain (or cause the Indirect Cloud Provider to provide and maintain) the necessary features, functionality, and tools. In addition, the financial institution should consider a flow down provision in the Service Agreement, requiring the MPS Vendor to contractually obligate its Indirect Cloud Provider to provide the features, functionality and tools for the use case and ensure that they work properly, enabling the MPS Vendor to meet its obligations to the financial institution in a manner that satisfies the financial institution's requirements. Discussion of other flow down provisions financial institutions may want to consider requiring in their Service Agreements can be found in **Section 4 (Subcontracting)** and other sections of this paper.[30]

## 3. Contract Terms

Regulators generally expect that financial institutions will consider, depending on the degree of risk and complexity of the third-party relationship, the inclusion of several specific provisions in their Service Agreements to facilitate effective risk management and oversight.[31] For the reasons discussed above, this paper presumes that Cloud Providers and their Cloud Services are of higher risk to financial institutions. As such, all of the suggestions and considerations discussed in this paper are relevant to any particular Cloud Service or Cloud Provider relationship and Regulators will generally expect them to be addressed in the relevant Service Agreement.

Because both the levels and types of risks may change over the lifetime of third-party relationships, financial institutions are advised by Regulators to review their Service Agreements periodically or upon learning of a change in a Cloud Provider relationship that impacts the risk profile of the relationship or services.[32] Changes that may trigger such review vary but include, for example, the deployment of new technology, the imposition of new

[30] "Misconfiguration of cloud resources is a prevalent cloud vulnerability and can be exploited to access cloud data and services. System vulnerabilities can arise due to the failure to properly configure security tools within cloud computing systems." FFIEC Joint Statement, *supra* note 7, at 5 (footnote omitted).

[31] DORA, *supra* note 4, at Article 30 stipulates key contractual requirements that must be included in agreements with ICT third-party service providers. OSFI Guideline B-10, *supra* note 6 at § 2.3, provides that an FRFI "should structure its written agreement with the third party in a manner that allows it to meet the expectations set out in this Guideline. OSFI expects the FRFI to include in written agreements for high-risk and critical arrangements the provisions that are set out in *Annex 2* of this Guideline". *See also* IIROC Outsourcing Guidance, *supra* note 6, at § 2.2, and Office of the Comptroller of the Currency, OCC Bulletin No. 2017-7, Supplemental Examination Procedures for Risk Management of Third-Party Relationships (2017) (hereinafter "OCC Bulletin 2017-7") (available at: https://www.occ.gov/news-issuances/bulletins/2017/pub-third-party-exam-supplemental-procedures.pdf) at 13.

[32] 2023 Interagency Guidance, *supra* note 12, at 935, discussing "Ongoing Monitoring".

regulatory requirements or a change in the structure of the Cloud Provider relationship (*e.g.*, by merger or other corporate action or a change in the nature of services provided).[33] Accordingly, Cloud Providers should expect that the financial institution may, from time to time, seek amendments to the Service Agreement to ensure effective and timely management of such risks.

### A. Subcontracting

Regulators expect that, as part of a financial institution's effort to identify whether any subcontracting arrangements pose additional or heightened risk to the financial institution, the financial institution will evaluate the volume and types of subcontracted activities, as well as the degree of the Cloud Provider's reliance on subcontractors.[34] This typically includes an assessment of the Cloud Provider's ability to identify, manage and mitigate risks associated with subcontracting including, among other things, how it selects and oversees its subcontractors and ensures that its subcontractors implement effective controls.

Service Agreements typically address when and how the Cloud Provider should notify the financial institution of its use, or intent to use, a subcontractor and the extent using specific subcontractors or subcontracting specific types of activities may be prohibited.[35] More detailed contractual obligations, such as reporting on subcontractors' conformance with performance measures, periodic audit results and level of compliance with laws and regulations are expected of financial institutions with respect to subcontracting arrangements integral to the activity being performed for the financial institution. Another important consideration addressed in the Service Agreement is whether assignment, transfer or subcontracting of the Cloud Provider's obligations to another entity without the financial institution's consent should be prohibited. Financial institutions may expect the right to terminate the contract without penalty if the Cloud Provider's subcontracting arrangements do not comply with contractual or legal obligations, or the Service Agreement is assigned without the financial institution's consent.[36]

Financial institutions are required by law to conduct their activities in a safe and sound manner, as well as, in compliance with applicable laws and regulations, and should therefore consider requiring that their Service Agreements obligate Cloud Providers to, and cause their subcontractors to, operate and maintain the services in accordance with the requirements of the laws, regulations and regulatory guidance applicable to the financial

[33] *See* § 3.B. (Comprehensive Information Sharing) of this paper for examples of other events that may trigger review. *See also* OSFI Guideline B-10, *supra* note 6, at § 2.4.1.
[34] 2023 Interagency Guidance, *supra* note 12, at 931 discussing "Reliance on Subcontractors".
[35] DORA, *supra* note 4, at Article 30(2)(a) requires that the contract contains "a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting". OSFI Guideline B-10, *supra* note 6, at § 2.2.4, as well as Annex 2 subsection (c).
[36] DORA, *supra* note 4, at Article 28(7) sets out circumstances, in relation to which, the contract with a service provider must provide the financial entity with a right to terminate. These include, for example, a "significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms".

institution or the services.[37] For the same reasons, financial institutions should consider requiring Cloud Providers to remain fully liable for the acts and omissions of their subcontractors and maintain written agreements with all or certain subcontractors that incorporate terms that protect the financial institution at least as much as the terms of the Service Agreement (including obligations relating to audit, security, confidentiality, privacy, compliance, business continuity and disaster recovery).[38]

Financial institutions also may want the Service Agreement to include an obligation by the Cloud Provider to maintain specified controls commensurate with the risks associated with the Cloud Provider's use of subcontractors. For example, such controls may mitigate risk associated with a subcontractor's location,[39] the Cloud Provider's dependency on a subcontractor for multiple activities or the subcontractor's failure to perform where such failure to perform has a material impact on the Cloud Provider's performance or on the financial institution's use of the services.[40]

Cloud Providers may resist accepting some of the contractual obligations that financial institutions deem necessary to have in place to effectively manage risk and meet regulatory expectations. For example, financial institutions recognize that it would be difficult for a Cloud Provider to seek and obtain prior written approval for use of all subcontractors from all financial institutions that use Cloud Services either directly or through an Indirect Cloud Provider. The Cloud Provider makes subcontractor decisions that it believes benefit all of its customers in terms of service levels and costs and therefore may resist giving each financial institution an effective right to veto otherwise acceptable subcontractors. This is equally true in the case of Indirect Cloud Providers.

Under appropriate circumstances, a financial institution may agree to forego the right to pre-approve subcontractors. Such decision by the financial institution should be based on its assessment of the risks associated with the subcontractor's activities and mitigating risk factors, such as contractual commitments by the Cloud Provider that help the financial institution effectively manage such risk within the financial institution's risk profile. This assessment is particularly important when the subcontracting arrangement includes higher risk activities, such as the provision of Indirect Cloud Services. Contract commitments may include, at a minimum, obligations for the Cloud Provider, including any MPS Vendor, to provide significant advance notice of its intent to use a subcontractor that the financial institution deems material (*e.g.*, an Indirect Cloud Provider or subcontractors based on their location), a demonstration of its ability to conduct — and report the results of — the necessary due diligence on the

[37] 2023 Interagency Guidance, *supra* note 12, at 932, commenting "Responsibilities for Providing, Receiving and Retaining Information" and "Responsibility for Compliance with Applicable Laws and Regulations."

[38] OCC Bulletin 2017-7, *supra* note 31, at 13; 2023 Interagency Guidance, *supra* note 12. *See also* FFIEC, Information Technology Examination Handbook, Audit Booklet (2012), (*available at* https://ithandbook.ffiec.gov/media/cmobvelk/ffiec_itbooklet_audit.pdf), (hereinafter "FFIEC Audit Booklet") at 18: "Financial institutions are required to effectively manage their relationships with key [technology service providers]" through means such as "[d]irectly auditing the [technology service provider's] operations and controls[;] […] [e]mploying the services of external auditors to evaluate the [technology service provider's] operations and controls; or [r]eceiving from, and reviewing sufficiently detailed independent audit reports on, [sic] the [technology service provider]." *Id*.

[39] 2023 Interagency Guidance, *supra* note 12, at 931, discussing "Reliance on Subcontractors".

[40] FFIEC Handbook, *supra* note 8, at 14; OCC Bulletin 2017-7, *supra* note 31, at 13.

new subcontractor and a willingness to assist the financial institution to itself conduct the necessary due diligence on the new subcontractor.[41] In lieu of a right to pre-approve all subcontractors, a financial institution may consider accepting a right to terminate the Service Agreement, without penalty, in the event the financial institution finds such new subcontractor unacceptable or the Cloud Provider fails to perform its subcontractor-related obligations or meet certain qualifications set forth in the Service Agreement (*e.g.*, a subcontractor cannot be a competitor of the financial institution).[42]

Relying on the right to terminate to mitigate risk is a challenging approach for the financial institution in many circumstances (*e.g.*, where the financial institution has made a substantial investment in transitioning to the Cloud Services or where termination and transition to a replacement Cloud Provider or an in-house solution may require a protracted period to complete) as it leaves termination of the contract as the financial institution's only remedy.

Where the privacy laws of the European Economic Area, Switzerland and/or the United Kingdom are applicable, even if it is not required that each new subcontractor must be specifically pre-approved in advance, the financial institution must have the right to receive notification of, and have a right to object to, each new subcontractor that is engaged.[43]

Moreover, the introduction of new subcontractors may also raise complex compliance issues, including when new subcontractors are located outside the country of the financial institution and their use involves the cross-border transmission of regulated data.

Financial institutions look for Cloud Providers willing to commit to the contractual considerations discussed in this Section and elsewhere in this paper, and this is generally true whether they contract with Cloud Providers to receive Cloud Services directly or with a MPS Vendor to receive Indirect Cloud Services. In the context of Indirect Cloud Services, financial institutions generally hold MPS Vendors liable for the services performed by Indirect Cloud Providers and require MPS Vendors to flow down their contractual commitments in the applicable Service Agreements to the Indirect Cloud Providers.

### B. Comprehensive Information Gathering.

Financial institutions typically expect that Service Agreements will include contractual commitments by the Cloud Provider to retain and provide — via periodic audit, questionnaire and reporting — accurate, timely and comprehensive information to the financial institution necessary to monitor risks and the Cloud Provider's

[41] OSFI Guideline B-10, *supra* note 6, at § 2.2.4.2 and Annex 2 subsection (c).
[42] 2023 Interagency Guidance, *supra* note 12, at 934 discussing "Subcontracting".
[43] The EU General Data Protection Regulation (Regulation (EU) 2016/679), (available at: http://data.europa.eu/eli/reg/2016/679/oj), (hereinafter "GDPR") at Article 28(3)(2) requires the contract to stipulate that the processor "shall not engage another processor without prior specific or general written of the controller". Note that the domestic legislation of Switzerland and the United Kingdom generally impose substantively equivalent data protection requirements to those stipulated by the GDPR.

performance and compliance with laws and regulations applicable to the Cloud Services.[44] The Service Agreements will likely address, to the extent appropriate on a risk basis: (i) the financial institution's ability to access its data, as well as access and use the Cloud Provider's data (and how such data and supporting documentation may be shared with Regulators as part of the supervisory process); (ii) the Cloud Provider's rights to access and use the financial institution's data (including associated metadata)[45] and/or systems (including those of its affiliates); (iii) notice of compliance lapses or other Cloud Provider events (*e.g.*, enforcement actions, regulatory proceedings) that pose a significant risk to the financial institution or its customers; (iv) notice of Cloud Provider's strategic or operational changes (*e.g.*, mergers, acquisitions, divestitures, use of subcontractors, key personnel changes or other business initiatives) that could affect the activities involved; and (v) the type and frequency of reports (performance reports, financial reports, security reports and control assessments) to be received from the Cloud Provider.[46]

In addition, financial institutions may expect Cloud Providers (and their subcontractors) to contractually commit to provide information reasonably requested by the financial institution on a periodic basis, or upon reasonable request, in connection with the provision of the Cloud Services to the financial institution (*e.g.*, response and completion of security questionnaires as well as Cloud Provider's independently audited financial condition). Cloud Providers should consider making available to their clients who serve as MPS Vendors, supporting information that would allow such MPS Vendors to demonstrate to their financial institution customers that any use and configuration of any Indirect Cloud Services relied upon by the MPS Vendor in providing services to the financial institution, substantially conform to the commitments made by the MPS Vendor to financial institutions under the relevant Service Agreement.

### C. Financial Institution Audit Rights

Depending on the level of risk and complexity associated with the Cloud Services, financial institutions will likely expect the unfettered and unconditional right to conduct audits, including initial and ongoing due diligence risk assessments or business performance reviews of a Cloud Provider's (and its subcontractors') premises, data centers and systems, as necessary, to verify and ensure compliance with the Service Agreement and applicable laws and regulations (*e.g.*, no restrictions or limits on access to certain locations or records or access to staff and

[44] 2023 Interagency Guidance, *supra* note 12, at 932 commenting "The Right to Audit and Remediation"; OSFI Guideline B-10, *supra* note 6, at § 2.3.3. In addition, under OSFI Guideline B-10, *supra* note 6, at Appendix 2 subsection (h), OSFI expects Service Agreements to require vendors to notify the FRFI of "(i) incidents/events (at the third party or a subcontractor) that impact or could impact services provided, the FRFI's customers/data or the FRFI's reputation; (ii) technology and cyber security incidents (at the third party or a subcontractor) to enable the FRFI to comply with its reporting requirements under OSFI's Technology and Cyber Security Incident Reporting Advisory dated August 16, 2021 (hereinafter the "Advisory"); (iii) changes in ownership of the third party; (iv) significant organizational/operational changes; and (v) material non-compliance with regulatory requirements (i.e. regulatory enforcement) or litigation." *See also* GDPR, *supra* note 43, at Article 28(3)(h) which requires that the contract between the controller and processor stipulates that the processor shall make available "all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."

[45] 2023 Interagency Guidance, *supra* note 12, at 932.

[46] *Id*. at 930, *et seq*.

external auditors; no obligation for a Regulator to undergo intermediary actions prior to exercising its right to audit; no limit on frequency, duration or the like).[47]

Whether an audit is required by the financial institution, and if so, the scope of the audit, typically depends on the risks associated with the contemplated use case of the financial institution.[48] The financial institution will typically consider whether the audit should include, among other things, cybersecurity programs, disaster recovery and business continuity plans, as well as the types and frequency of testing of such programs and plans. In addition, the financial institution will likely expect the Cloud Provider to remediate all material vulnerabilities identified by an audit within a defined period of time based on their criticality and include a right by the financial institution to terminate, without penalty, in the Service Agreement for the Cloud Provider's failure to meet its obligation to remediate.

Although it may be challenging for Cloud Providers to provide all customers with the right to conduct on-site inspections and audits on data centers and systems, Regulators expect financial institutions to apply sound risk management principles to the management of their third-party risk exposure in a manner that is commensurate with the level of risk, complexity and size of the financial institution and the nature of their third-party relationships. Such approach typically leads financial institutions to require Cloud Providers to grant broad audit rights to the financial institution, applicable to both Cloud Providers and their subcontractors.

In addition, Regulators expect that a financial institution's Cloud Providers (and their subcontractors) will provide cooperation and assistance upon request, and, at minimum, provide information requested by Regulators in connection with the provision of services to financial institutions (see, in addition, **Section 3.J (Books and Records)** below).[49]

As discussed earlier, financial institutions may want to assess an Indirect Cloud Provider as if they were the financial institution's direct Cloud Provider and require the MPS Vendor to contractually obligate the Indirect Cloud Provider

---

[47] *See* Final Report on, EBA Guidelines on outsourcing arrangements (EBA/GL/2019/2), European Banking Authority (Feb. 25, 2019) (available at: https://www.eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.pdf/38c80601-f5d7-4855-8ba3-702423665479) paragraph 87(a), stating that for outsourcing of critical or important functions, the written agreement with the vendor has to grant the financial institutions and the regulators, full access to all relevant business premises (*e.g.*, head offices and operation centers), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors.; OSFI Guideline B-10, *supra* note 6 at § 2.3.3, which provides that "The FRFI's third-party arrangements should allow the FRFI timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks. The FRFI should also have the right to conduct or commission an independent audit of a third party." *See also* Directive 2014/65/EU (2014), at Art. 2, § 1-4, (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN) (hereinafter "MiFID"). *See also*, GDPR, *supra* note 43, and DORA, *supra* note 4, at Article 30(3)(e). "[C]ontract provisions [addressing a banking organization's] audit and oversight rights] may also reserve the banking organization's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits." 2023 Interagency Guidance, *supra* note 12, at 932.

[48] DORA, *supra* note 4, at Article 28(6) provides that "in exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards."

[49] *See, e.g.*, 17 C.F.R. § 240.17a-1. OSFI Guideline B-10, *supra* note 6, at §§ 2.3.2.2 and 2.3.3.3.

to comply with all of the MPS Vendor's obligations in the Service Agreement to ensure the MPS Vendor's compliance with the Service Agreement with respect to the subcontracted Cloud Services, including, the types of contractual provisions discussed in this Section.

### D. Cloud Provider Self-Audit and Reports

In addition to a financial institution's right to conduct audits on the Cloud Provider itself as discussed in the foregoing **Section C (Financial Institution Audit Rights)**, financial institutions expect Cloud Providers, Indirect Cloud Providers and their other subcontractors to perform self-audits on a periodic basis and provide those audit reports to the financial institutions.

Financial institutions typically request the Cloud Provider to provide a copy of the resulting report, such as a SOC 2 Report.[50] If the financial institution reasonably believes that the SOC 2 Report does not address requirements set out in the Service Agreement, the financial institution may require the Cloud Provider to include those requirements in the next audit and report.[51] To address the risk that a report identifies any material non-compliance, the financial institution typically requires that the Service Agreement includes a specific time period for remediation and termination rights, exercisable without penalty, if the Cloud Provider fails to resolve the issue within the time period prescribed.[52]

### E. Information Security and Cybersecurity of Customer Data

Regulators generally expect Service Agreements to: (i) contain comprehensive information security requirements on Cloud Providers and their subcontractors commensurate with the risks intended to be addressed by such provisions; and (ii) satisfy the applicable requirements laid down by privacy and cybersecurity laws and regulations.[53] This includes requiring Cloud Providers to have policies and procedures in place to ensure the confidentiality, security, integrity and availability of the data of financial institutions and their clients, employees and others ("**Customer Data**"), including Customer Data stored or transmitted on the Cloud Providers' and their

[50] System and Organization Controls known as "SOC" refers to a suite of reports that may be producing during an audit in accordance with standards laid down by the American Institute of Certified Public Accountants (AICPA). A SOC 2 Report results from reporting carried out in accordance with particular criteria established by the AICPA to review specific types of controls; OSFI Guideline B-10, *supra* note 6, at § 2.3.3.
[51] 2023 Interagency Guidance, *supra* note 12, at 932 discussing "The Right to Audit and Remediation."
[52] FFIEC Handbook, *supra* note 8, at 13; 2023 Interagency Guidance, *supra* note 12, at 932 discussing "The Right to Audit and Remediation" DORA, *supra* note 4, at Articles 28(6) and (7).
[53] *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 *et seq*.; FFIEC Handbook, *supra* note 8, at 26; OCC Bulletin 2017-7, *supra* note 31, at 13; Guideline B-10, *supra* note 6, at § 2.3.2. *See also*, DORA, *supra* note 4, at Article 28(5) which states "Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards." *See also*, the contractual requirements for agreements with "processors" set out at Article 28(3) GDPR *supra* note 43. *See also*, the contractual requirements for agreements with "service providers", "contractors" and "third parties" under the California Consumer Privacy Act of 2018, Civ. Code, § 1798.100 *et seq*., added by Stats. 2018, ch. 55, § 3, eff. Jan. 1, 2020, as subsequently amended by the California Privacy Rights Act of 2020.

subcontractors' systems.[54] In addition, Regulators expect Service Agreements to include specific provisions relating to the Cloud Providers' and their Indirect Cloud Providers subcontractors' administrative, technical, organizational and physical controls necessary to safeguard Customer Data and their systems against unauthorized access, use, disclosure, modification, unavailability and deletion and unavailability, including requiring Cloud Providers to flow such provisions down to their subcontractors.[55] As a result, financial institutions look for Cloud Providers willing to commit to these requirements, whether they are contracting directly with a financial institution or with a MPS Vendor that provides services directly to financial institutions.

Cloud Providers commonly seek to satisfy these requirements by agreeing to maintain an environment and internal controls consistent with their then-current SOC 2 Report and by including specific requirements in the Service Agreement. MPS Vendors may commit to maintaining the environmental and internal controls to the extent permissible by their Indirect Cloud Providers. Based on the contemplated use case and a risk-based analysis, financial institutions may consider seeking to include certain commitments by the Cloud Provider in the Service Agreement, including, at a minimum, appropriate controls regarding their Indirect Cloud Providers, personnel and subcontractors (especially those that may access Customer Data) and their systems and infrastructure.[56]

The Cloud Provider, as service provider to both financial institutions and their vendors, should consider being contractually responsible for all of the appropriate controls unless its Service Agreements with either financial institutions or the other vendors expressly state that the Cloud Provider is not responsible, in which case the Cloud Provider should consider contractually agreeing to provide and maintain the features, functionality and tools that allow financial institutions and their vendors to appropriately configure the Cloud Services in a manner that satisfies risks associated with use of the Cloud Services, such as security and data location. The Cloud Provider should also consider agreeing to provide ample notice and detailed information regarding any changes to the Cloud Services' features, functionality, and tools.

Financial institutions expect the Cloud Provider to be liable and responsible for any failures in the features, functionality, and tools of Cloud Services. Cloud Providers will typically conduct regular penetration tests on their systems to validate that the systems are adapting to the latest threats.[57] Cloud Providers should consider sharing such results (including those of tests of their subcontractors' systems) and permitting financial institutions to conduct

[54] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11; 2023 Interagency Guidance, *supra* note 12, at 933 discussing "Confidentiality and Integrity"; OCC Bulletin 2017-7, *supra* note 31, at 13; GDPR, *supra* note 43, at Article 32. OSFI Guideline B-10, *supra* note 6, at § 2.3.2, Annex 2 subsection (f) and Annex 2 subsection (g); IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 2, Topic 3 and Topic 4.

[55] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11; FFIEC Handbook, *supra* note 8 at 12; OCC Bulletin 2017-7, *supra* note 31, at 13; GDPR, *supra* note 43, at Article 28(3)(c) requires that the contract stipulates that the subprocessor will take all technical and organizational measures required under Article 32 and, note also that where the EU Standard Contractual Clauses are used (to legitimate cross-border transfers of data outside of the European Economic Area), it is a requirement to list out the relevant technical and organizational measures implemented to protect personal data; *see also id.* at Article 28(3)(f).

[56] *See* N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.05, 500.12, 500.14, 500.15; FFIEC Handbook, *supra* note 8, at 18-22, 24 and 29; FFIEC BCM, *supra* note 8, at § V, "Business Continuity Plan"; Interagency Guidance, *supra* note 8, at "Qualifications, Backgrounds, and Reputations of Company Principals" and "Ongoing Monitoring"; OCC Bulletin 2017-7, *supra* note 31, at 13, 14-15.

[57] *Id*.

their own penetration testing.[58] Financial institutions may be willing to agree to certain conditions to conduct their own penetration testing so long as those conditions are specifically set out in the Service Agreement and the Cloud Provider agrees to provide ample notice of changes to allow the financial institution to assess the impact of such changes. In the event any penetration tests reveal deficiencies, financial institutions expect the Cloud Provider to commit to tracking and remedying such deficiencies within a prescribed time frame appropriate for the criticality of the deficiency.[59]

Cloud Providers should consider, at least once annually, providing financial institutions with a written attestation signed by an officer of the Cloud Provider stating that the Cloud Provider complies with its security obligations. Also, upon request, the Cloud Provider may arrange for appropriate personnel of the Cloud Provider to review and discuss the underlying details of such attestation with the financial institution.

### F. Security Breach Notification and Remediation

Regulators require financial institutions to notify the Regulators of any unauthorized access, use, modification, deletion, or unavailability of Customer Data or if there has been unauthorized access or use of their services or financial institutions' systems (each, a "**Cybersecurity Event**").[60]

The Service Agreement should specify when and how the Cloud Provider will disclose, in a timely manner, Cybersecurity Events, including, information security breaches or unauthorized intrusions.[61] Considerations may include the types of data stored by the Cloud Provider, legal obligations for the financial institution to disclose the breach to its Regulators, customers or other affected persons (including, within any legally prescribed timeframes for disclosure),[62] the potential for consumer harm, or other factors. Financial institutions typically expect Cloud Providers to provide notice of the Cybersecurity Event to the financial institution within a timeframe that allows the financial institution to comply with applicable laws and regulations. Such notice should be in writing (including to

[58] *Id*.
[59] *Id*.
[60] OCC Bulletin No. 2005-13, Response Programs for Unauthorized Access to Customer Information and Customer Notice – Final Guidance: Interagency Guidance (2005), https://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-13.html, at "Ongoing Monitoring" (hereinafter OCC Bulletin 2005-13); FFIEC Handbook, *supra* note 7, at 13; OCC Bulletin OCC Bulletin 2017-7, *supra* note 31, at 13; OSFI Guideline B-10, *supra* note 6, at § 2.4.2 and Annex 2 subsection (h), pursuant to which the FRFI should be made aware of "technology and cyber security incidents [(at the vendor or a subcontractor)] to enable the FRFI to meet its reporting requirements under [the Advisory]; IIROC Rule 3703 and Guidance Note GN-3700-22-001 "Compliance with IIROC's Cybersecurity Incident Reporting Requirements" dated February 10, 2022 (hereinafter "IIROC Cyber Incident Guidance"); *Personal Information Protection and Electronic Documents Act* (Canada) (S.C. 2000, c. 5) (hereinafter "PIPEDA"), including the Breach of Security Safeguards Regulations (SOR/2018-64), where, under § 10.1 of PIPEDA, notification to the Privacy Commissioner of Canada is required where there has been "any breach of security safeguards involving personal information under [an organization's] control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual."; GDPR, *supra* note 43, at Article 33(1) requires notification of a data breach to the applicable supervisory authority within 72 hours unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons[.]"
[61] GDPR, *supra* note 43, at Article 33(2) requires that the processor "notify the controller without undue delay after becoming aware of a personal data breach."; OSFI Guideline B-10, *supra* note 6, at § 2.4.2.2, which provides that Service Agreements "could include, among other things, requirements to promptly notify the FRFI of technology and cybersecurity incidents (at the third party or the subcontractor) including providing information on each incident in line with the [Advisory]." *See also* IIROC Cyber Incident Guidance, *supra* note 60.
[62] *See*, generally, *supra* note 60.

an email address approved by the financial institution), however, in some instances it may be appropriate for notification to also be made by telephone, and should include all material details of the Cybersecurity Event, including, among other things, estimates of the effects on the financial institution and its customers, as well as corrective action to be taken by the Cloud Provider. In some cases, an initial notification should be made containing available information, with further information provided as it becomes available. In addition, the Cloud Provider should consider committing to promptly contain, control, and remediate any Cybersecurity Event (including providing notices to individuals and payment for credit monitoring, as required by applicable law). The Cloud Provider should also consider providing the financial institution, upon request, with updates to the investigation and resolution of the Cybersecurity Event, while also indemnifying the financial institution and being liable for the financial institution's costs and other damages arising from the Cybersecurity Event.[63]

For MPS Vendors that rely on Indirect Cloud Providers to provide services directly to financial institutions, any unauthorized access or use of the Cloud Services could constitute a Cybersecurity Event. Therefore, in the agreement between the MPS Vendor and Indirect Cloud Provider, the Indirect Cloud Provider should consider agreeing to provide prompt notice and detailed information regarding any Cybersecurity Event to assist the MPS Vendor to meet their obligations to financial institutions.[64]

### G. Disaster Recovery and Business Continuity

Regulators expect financial institutions to take steps to ensure business resilience.[65] When a financial institution engages a Cloud Provider, Regulators expect that the financial institution will assess how the Cloud Provider will maintain continuity of its services so that the financial institution is able to maintain continuity and resilience of the financial institution's overall operations.[66]

Financial institutions expect to enter into Service Agreements that impose comprehensive disaster recovery and business continuity requirements on Cloud Providers including maintaining appropriate controls to support operational resilience of the services, such as protecting and storing programs, backing up datasets, addressing cybersecurity issues and maintaining exit strategies, as more fully detailed in **Section 3.L (Termination, Non-**

[63] "An assessment of a third party's operational resilience practices supports a banking organization's evaluation of a third party's ability to effectively operate through and recover from any disruption or incidents, both internal and external. Such an assessment is particularly important where the impact of such disruption could have an adverse effect on the banking organization or its customers, including when the third party interacts with customers." 2023 Interagency Guidance, *supra* note 12, at 934 discussing "Operational Resilience". "Review and consideration of a third party's incident reporting and management processes is helpful to determine whether there are clearly documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents." *Id.* discussing "Incident Reporting and Management Processes". N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.16, 500.17 (a) and (c).

[64] OCC Bulletin 2005-13, *supra* note 8.

[65] 2023 Interagency Guidance, *supra* note 12, at 933 discussing "Operational Resilience and Business Continuity".; OSFI Guideline B-10, *supra* note 6, at § 2.3.4 and Annex 2 subsection (k); DORA, *supra* note 4, at Article 10.

[66] *Id*; OCC Bulletin 2017-7, *supra* note 31, at 13; OSFI Guideline B-10, *supra* note 6, at §§ 2.3.4, 2.3.5 and Annex 2 subsection (k); IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 2, Topic 3 and Topic 6.

**Renewal and Suspension)**, below.[67] This includes requiring Cloud Providers to implement and maintain current and sound disaster recovery and business continuity plans and provide financial institutions with operating procedures to be carried out in the event business continuity plans are implemented, including specific recovery time and recovery point objectives.[68] In addition, Service Agreements may also stipulate whether and how often the financial institution and the Cloud Provider will participate in the Cloud Provider's tests of their business continuity plans. Cloud Providers that perform critical functions for the financial institution may be expected by the financial institution to participate in the financial institution's testing of its business continuity plan for such functions. Financial institutions also expect to be notified of the outcome of the vendor's tests, and to review the results of the tests.[69] Further, Cloud Providers are expected to remediate any issues discovered during these tests.

Some Cloud Providers are now insisting on exclusivity provisions during the term of the Service Agreement, obligating the financial institution to engage only the contracting Cloud Provider for the contracted services. Financial institutions are advised to bear in mind that, in an engagement for Cloud Services, an exclusivity provision may impact the ability of a financial institution to fulfill its regulatory obligations with regard to disaster recovery and business continuity planning. Exclusivity provisions would prevent the institution from having an alternate provider in the event of a disaster impacting the contracting Cloud Provider or prevent the institution from negotiating and entering into a contract with a replacement vendor prior to expiration of the current contract.

In addition, some Cloud Providers are now using very broad force majeure provisions that would permit the Cloud Provider to easily avoid most performance obligations. These provisions should be narrowly drafted and be balanced by requirements for the Cloud Provider to design, test and operate business continuity/disaster recovery and resilience measures. A pandemic, for example, may be a force majeure event, but it should not be used as a *carte blanche* excuse for non-performance and the Cloud Provider should have a pandemic response plan in place. It is advisable that force majeure provisions should contain language requiring an equitable adjustment in fees during the period in which performance was impacted and language permitting the financial institution to terminate the Service Agreement without penalty.

Cloud Providers often resist the ability of financial institutions to participate in business continuity plan testing. Cloud Providers may, instead, agree to provide only summaries of their business continuity plans and test results, citing security and confidentiality reasons for refusing to permit their customers to participate in plan testing or to review the full details of their plans and test results. Financial institutions will use a risk-based approach to determine if a

[67] FFIEC BCM, *supra* note 7 at § IV(A)(5), "Third-Party Service Providers;" OCC Bulletin 2017-7, *supra* note 31, at 13; *id*. at § (E); FFIEC Handbook, *supra* note 7, at 12 and 15; ]; 2023 Interagency Guidance, *supra* note 12, at 932-933, discussing "Performance Measures or Benchmarks" and "Operational Resilience and Business Continuity"; OSFI Guideline B-10, *supra* note 6, at §§ 2.3.4, 2.3.5 and Annex 2 subsection (k). *See also*, DORA, *supra* note 4, at Article 28(8) which stipulates that the financial entity must have in place "exit strategies" for "ICT services supporting critical or important functions".

[68] FFIEC BCM, *supra* note 8, at § VII(I), "Third-Party Service Provider Testing".

[69] 2023 Interagency Guidance, *supra* note 12, at 933 discussing "Operational Resilience and Business Continuity"; OSFI Guideline B-10, *supra* note 6, at § 2.3.4 and Annex 2 subsection (k).

Cloud Provider's business continuity contractual commitments are sufficient in light of the risks associated with the nature of the Cloud Provider's service and the scope of the data provided to the Cloud Provider. Gaps often exist between what financial institutions view as appropriate and what Cloud Providers are willing to agree to contractually.

Financial institutions expect that MPS Vendors will commit to configuring their Indirect Cloud Services in a manner that enables them to meet their business continuity obligations to the financial institutions.[70] That also means that Indirect Cloud Providers should have a contractual obligation to provide and maintain the necessary functionality to assist those MPS Vendors to meet their business continuity obligations to financial institutions.

### H. Confidentiality

Financial institutions expect to include in their Service Agreements confidentiality obligations designed to protect their confidential information,[71] especially protecting material non-public information ("**MNPI**", also known as "insider information"),[72] maintaining any required information barriers[73] and protecting commercially sensitive information such as trading algorithms and client data. The Service Agreement should, at a minimum, prohibit the Cloud Provider and its subcontractors from using or disclosing the financial institution's confidential information (which is generally broadly defined) except as necessary to provide the contracted activities or comply with legal requirements, and obligate the Cloud Providers to protect the confidential information with appropriate security measures and notify the financial institution of any disclosure or misuse.[74]

Financial institutions expect that the confidentiality obligations cover all the financial institution's confidential information, regardless of whether and where it is processed and stored by the Cloud Provider. Therefore, those obligations should also cover, for example, information about the financial institution's use cases, customers, and pricing, including information obtained when providing professional services or support to the financial institution (such as access information, credentials and log-in information, as well as any resulting derivatives and analytics). Although it is common to exclude certain types of information from the Cloud Provider's confidentiality obligations (*e.g.*, publicly available information, information already known by the Cloud Provider), these exclusions generally do not apply to Customer Data.

Financial institutions may also obtain confidential information about the Cloud Provider when receiving services

[70] FFIEC Handbook, *supra* note 8 at 14.
[71] *Id*. at 13; 2023 Interagency Guidance, *supra* note 12, at 933 discussing "Confidentiality and Integrity"; OCC Bulletin 2017-7, *supra* note 31 at 13; OSFI Guideline B-10, *supra* note 6 at § 2.3.2 and Annex 2 subsection (g).
[72] See UK Financial Conduct Authority, *Best practice note - Identifying, controlling and disclosing inside information* (Jun. 9, 2020, last updated Jan. 1, 2023) (available at: https://www.fca.org.uk/markets/best-practice-note-identifying-controlling-and-disclosing-inside-information.
[73] *See* Security and Exchange Commission, Press Release, *SEC Charges Virtu for False and Misleading Disclosures Relating to Information Barriers* (Sep. 12, 2023) (available at: https://www.sec.gov/news/press-release/2023-176) describing charges against a broker-dealer relating to information barriers.
[74] FFIEC Handbook, *supra* note 8, at 13; 2023 Interagency Guidance, *supra* note 12, at 933 discussing "Confidentiality and Integrity"; OCC Bulletin 2017-7, *supra* note 31, at 13.

from the Cloud Provider. This may include information regarding how the Cloud Provider's services work, including reports describing the Cloud Provider's security measures and business continuity plans. While it is generally acceptable for the financial institution to undertake confidentiality obligations relating to the Cloud Provider's confidential information, exceptions may be appropriate to the extent the financial institution provides services to clients, including those clients that are regulated entities. Those clients may also be required by applicable regulation to perform due diligence on the financial institution, including regarding the financial institution's use and configuration of Cloud Provider services, as well as obtain related reports. Therefore, the parties should consider including in Service Agreements express language permitting the financial institution to disclose certain aspects of the Cloud Provider's confidential information, such as information necessary to satisfy client due diligence requests or disclosure of information required by law or upon a Regulator's request.

### I. Compliance

Regulators are clear that it is important for a Service Agreement to: (i) specify the obligations of the Cloud Provider and the financial institution to comply with applicable laws and regulations (including relevant guidance and self-regulatory standards); (ii) provide the financial institution with the right to monitor and be informed about the Cloud Provider and its subcontractors' compliance with applicable laws and regulations; and (iii) obligate the Cloud Provider to timely remediation if issues arise.

### J. Books and Records

Cloud Providers may provide services that create, or electronically store, data which financial institutions must retain pursuant to regulation.[75] Regulators consider this data, which is commonly referred to as the financial institution's books and records ("**Books and Records**"), necessary to preserve the orderly operation of financial markets and protect investors.[76] For example, U.S.-registered broker-dealers are required to create certain Books and Records and either: (i) store them in a non-rewriteable, non-erasable manner (commonly referred to as "write once, read many" or "WORM" format) that can verify and serialize the Books and Records; or (ii) provide an audit trail alternative that meets the requirements of 17a-4.[77]

When leveraging a Cloud Provider's services, financial institutions are required to conduct due diligence on the Cloud Provider's services and provide Regulators with notification. The following are the types of considerations that financial institutions and Cloud Providers should consider regarding Books and Records requirements.

[75] *See, e.g.*, 17 C.F.R. §§ 240.17a-3 and 240.17a-4 (requiring regulated entities to make certain records. Books and Records include, among other things, communications relating to financial institutions' "business as such," trade blotters, financial ledgers, customer account ledgers, securities records, order tickets and trade confirmations); OSFI Guideline B-10, *supra* note 6, at § 2.3.2.2; IIROC Outsourcing Guidance, *supra* note 6 at Appendix A Topic 2.

[76] *Id*.

[77] The audit trail alternative became a viable alternative on January 3, 2023, following the effective date of amendments to Rule 17a-4.

### 1. Access to Books and Records

Regulators expect financial institutions to have facilities available for Regulators to readily access in a readable format those records that may be requested.[78] As a result, financial institutions and Cloud Providers should store Books and Records in a readily accessible format. Furthermore, the protocol by which the financial institution can access the Books and Records should be defined and constructed to limit access to parties approved by the financial institution only.

### 2. Ownership of Books and Records relating to Customer's business.

It is also important that financial institutions retain ownership of their data created or processed using SaaS providers since some SaaS providers seek to claim ownership of the financial institution's own books and records following the transition from on-premise software to SaaS solutions. The contractual provisions presented by vendors can be complex and merit carful legal review. Financial institutions should consider if they need an enduring license to use and adapt any proprietary formats or taxonomies used by vendors for structuring a financial institution's books and records.

### 3. Duplication and Other Redundancy Capabilities

Regulators generally require financial institutions to retain a duplicate copy of the Books and Records or an audit trail that will permit re-creation of the original record if it is modified or deleted.[79] Financial institutions will seek Cloud Provider solutions that have functionality that maintains synchronized Books and Records (typically in different locations), including the attending indexes, if applicable to the storage medium. Concurrently, Cloud Providers should consider providing and maintaining mechanisms for financial institutions to monitor the duplication process or provide sufficient documentation, including periodic testing, that the process is effective. Assurances by the Cloud Provider that the process is in place may include notification provisions for system outages, incomplete data duplication or other information that a financial institution may seek.

### 4. Deletion and Termination

Broker-dealers and financial institutions are required to retain Books and Records for various time periods.[80] Cloud Providers should expect to be asked and be prepared to provide financial institutions with the tools necessary to manage their Books and Records, including mechanisms to identify the type of Books and Records and apply the relevant retention period (including records subject to a legal hold). Under no circumstances should any Books and Records be deleted without the prior authorization of the financial institution. Additionally, in cases where the

[78] 17 C.F.R § 240.17a-4(f)(2)(iv) (requiring records in a human readable format and in a reasonably usable electronic format); OSFI Guideline B-10, *supra* note 6, at § 2.3.2.2.
[79] 17 C.F.R. § 240.17a-4(f)(2)(i).
[80] *See, e.g.*, 17 C.F.R. § 240.17a-4(a)-(e). Many records relating to a regulated entity's business must be preserved for a period of not less than six (6) years, while others must be retained for three (3) years or for the life of the enterprise.

deletion action rests with the Cloud Provider, clear documentation of the deletion method with certification that such deletion is complete and permanent and signoffs from the financial institution should be pre-determined.

In addition to ongoing regulatory requirements, Cloud Providers and financial institutions must have established protocols that apply if the Service Agreement expires or terminates. In almost every instance, the retention period of the Books and Records created by the Cloud Provider's solution will still be running. Given that financial institutions will not be able to delete or discard the Books and Records, the parties should consider an orderly transfer of the Books and Records to a new system. Practically speaking, this means that notice periods under the Service Agreement should be adequate for financial institutions to identify a new compliant storage solution for the Books and Records and transfer the Books and Records. The Service Agreement should provide that, notwithstanding any expiration or termination, the Cloud Provider should hold a copy of the Books and Records until the transfer is complete because deleting Books and Records for any reason, including due to non-payment, could potentially result in the Cloud Provider incurring secondary liability, abetting the financial institution in a violation of its regulatory requirements.[81]

### 5. Third Party Undertaking

Third parties that store Books and Records for broker-dealers in the United States must file a written undertaking that permits[82] Regulators to access and obtain copies of the Books and Records and there are similar safeguards for access by Regulators to Books and Records in other jurisdictions, including data residency requirements.[83] For financial institutions that maintain independent access to Books and Records, Cloud Providers may be required to undertake instead that they will not impede or prevent a Regulator's access.[84] Where the financial institution or a Cloud Provider uses the Cloud Provider's solution for a purpose that generates Books and Records that are required to be retained, Regulators may consider the Cloud Provider to be such a third party subject to these requirements. Further, if a Regulator contacts the Cloud Provider to request access or copies of records, the Cloud Provider should notify the financial institution.

Therefore, for financial institutions to comply with these regulations when implementing Cloud Providers' services, the Service Agreement should include language mandating the Cloud Provider to regularly disclose the timelines of its product development plans or other key milestones. Concurrently, Cloud Providers should agree to disclose

[81] *See, e.g.*, Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 96034, 87 FR 66412, 66429-30 (Nov. 3, 2022) ("Contractual provisions that would permit, among other things, a service provider to withhold, delete, or discard records in the event of non-payment by the broker-dealer are inconsistent with the retention requirements of Rule 17a-4 and the undertaking requirements of Rule 17a-4(i). Moreover, if a third party deletes or discards a broker-dealer's records in a manner that is not consistent with the retention requirements in Rule l7a-4, such action would constitute a primary violation of the rule by the broker-dealer **and may subject the service provider to secondary liability for causing or aiding and abetting the violation**.").

[82] 17 C.F.R. § 240.17a-4(i).

[83] UK Financial Conduct Authority, Finalised guidance FC 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT Services, (Jul. 2016, last updated Sep. 2019) (available at: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf) (hereinafter "FCA Guidance").

[84] 17 C.F.R. § 240.17a-4(i)(1)(ii).

such timelines to their customers that provide services to financial institutions. In addition, given the importance of the retention of data, the Service Agreement should include provisions addressing inadvertent deletion, including disclosure and remediation, where possible. As a practical matter, if a Cloud Provider is developing a solution for use by financial services firms, there are organizations that will provide a certification that can be used to demonstrate to a financial institution client, Regulator or audit team that the solution meets these requirements.

MPS Vendors that rely on Indirect Cloud Services to provide their services to financial institutions often have an obligation to configure the Indirect Cloud Services in a manner that enables them to meet obligations to their financial institution clients relating to Books and Records. That also means the Indirect Cloud Provider should consider obligations relating to making available the functionality to assist those MPS Vendors to meet their Books and Records obligations to financial institutions.

### K. Customer Data Controls

Regulators require financial institutions to maintain controls with regard to Customer Data appropriate to effectively manage risks associated with the receipt and handling of Customer Data by the Cloud Provider, its Indirect Cloud Provider or any of its other subcontractors, which typically includes backing up Customer Data, restricting the location where Customer Data is processed (including due to the growing number of data localization laws), knowing where Customer Data is stored, encrypting Customer Data in electronic form while "in transit", "at rest" or "in use", employing methodologies reflecting industry best practices (including standards from the US National Institute of Standards and Technology) and knowing who has access to it (including access to encryption keys).[85] As a baseline, therefore, Cloud Providers should require the Service Agreement to be explicit that the financial institution owns all Customer Data and ancillary and derivative data (including usage reports, tracing of users, etc.) and that the Customer Data may be used solely as necessary to render the services to the financial institution. Cloud Providers should also consider contractually committing to provide and maintain the features, functionality and tools that allow financial institutions to back up Customer Data, including where Customer Data will be processed and stored.[86] Given the potential for differences in laws from country to country, functionality that only allows for controls at the continent or region level is generally insufficient for financial institutions.[87] In addition, financial institutions may require Cloud Providers to specify the location(s) where Customer Data may be processed and stored in the Service Agreement and agree to not relocate Customer Data from the specified location(s) unless approved or directed by the financial institution.[88] For financial institutions to meet their ongoing monitoring obligations, Cloud Providers should provide the then-current locations where Customer Data is presently stored or processed at the

[85] *See* FFIEC Handbook, *supra* note 8, at 16; FFIEC BCM, *supra* note 8, at § IV(A); OSFI Guideline B-10, *supra* note 6, at § 2.3.2, Appendix 2 subsection (f) and Appendix 2 subsection (j).
[86] FFIEC Handbook, *supra* note 8, at A-5; OSFI Guideline B-10, *supra* note 6, at § 2.3.2.
[87] FFIEC Handbook, *supra* note 8, at C-5.
[88] *See* FFIEC Handbook, *supra* note 8, at 13. *See also*, FCA Guidance, *supra* note 83.

outset of the engagement, and upon the financial institution's request thereafter. Any change in location should be subject to the Cloud Provider's prior written approval in accordance with the notice requirements of the Service Agreement. Certain jurisdictions may require additional obligations and language to be added to Service Agreements.

Financial institutions typically require that access to Customer Data be limited solely to those who need access to provide the services to the financial institution and only for that purpose. That means the Service Agreement should limit access to certain personnel only and be subject to controls put in place by the Cloud Provider to ensure, maintain and enforce access entitlements. Furthermore, to the extent a Regulator or government entity requires the Cloud Provider to disclose Customer Data, the Service Agreement should specify the process, which should include compliance with applicable laws and appropriate due process.

With regard to MPS Vendors and Indirect Cloud Services on which they rely to provide their services to financial institutions, financial institutions may require those MPS Vendors to configure the Indirect Cloud Services in a manner that enables them to allow financial institutions to maintain appropriate controls with regard to Customer Data, including control over the location of that data. As a result, Indirect Cloud Providers should have an obligation to make available the functionality and information necessary to assist those MPS Vendors to meet their obligations to financial institutions.

As discussed above, technology in the cloud continues to evolve, becoming increasingly more complex. It is critical that financial institutions devote the necessary resources, with the necessary qualifications and expertise, to fully understand technology as it develops, along with the consequences of its use and its alignment, or not, with the financial institution's business strategy and associated risks. Today, for example, the importance of a clear and precise definition of the right to use Customer Data is particularly true with the growing risks associated with the use and integration of third-party artificial intelligence ("**AI**") tools by financial institutions and Cloud Providers, including open-source models, vendor platforms and commercial APIs. As the use and sophistication around artificial intelligence grows, financial institutions will likely seek to ensure that its personnel and external experts have the sufficient level of skill and expertise to assess risks posed by such technical developments and that Cloud Providers comply with the financial institution's applicable policies and procedures, such as guidelines for ethical AI development and monitoring and auditing protocols, including tailored assessments of the models themselves.

It is essential too that financial institutions be wary of Cloud Providers requesting broad use rights in Customer Data, typically phrased as a right to "use Customer Data for improvement of vendor's products and services" or to "use aggregated data derived from performance of the services". In many instances, such rights are either too broad or poorly defined in the Service Agreement. Customer Data may include MNPI and other commercially sensitive data, third party data which is subject to licensing restrictions, and PII/personal data subject to privacy laws — these factors are difficult to reconcile with use of the data by the Cloud Provider. If such rights are to be

granted, a clear definition of what the right means should be provided (*i.e.*, Customer Data shall be used to improve the existing functionality of the Cloud Provider's products only and not to: (i) train AI models; or (ii) market or commercialize existing or new products. Use of aggregated data includes only Customer Data, de-identified by the Cloud Provider and aggregated consistent with applicable law and such that the data is not capable through any means of being reidentified to any individual or entity). In addition, financial institutions may expect a Cloud Provider to assume full liability and indemnify the financial institution from any claims or damages that may result from use of Customer Data for reasons other than as required to perform the contracted services.

### L. Termination, Non-Renewal and Suspension by Cloud Provider

Operational certainty of the Cloud Services is paramount to financial institutions, particularly when they are deemed critical or of higher risk to the financial institution.[89] In engagements where availability of the Cloud Provider's services and access to Customer Data are essential, financial institutions expect that the Cloud Provider will not be able to quickly or easily terminate, suspend or not renew the services it provides to the financial institution.[90]

Financial institutions expect Service Agreements to include termination and notification provisions that allow for the orderly transition of Cloud Provider's services to an in-house solution or to another third party, in all cases, including when the Cloud Provider desires to terminate or not renew any portion of the services it provides to the financial institution. That means the Cloud Provider should be able to do so solely on appropriate notice to the financial institution that allows for the orderly transition of the activity, without prohibitive expense and with the following obligations:[91]

1. Provide transition assistance to financial institutions.
2. Provide for the appropriate and timely return and retrieval, and subsequent destruction and/or deletion, of Customer Data and/or other resources.
3. Assign all costs and obligations associated with transition and termination.
4. Provide the financial institution with continued access to and use of the Cloud Provider's services on an "as-is" basis for a reasonable period of time to ensure an orderly transition.
5. Enable the financial institution to terminate the relationship with reasonable notice and without penalty, if formally directed to do so by the financial institution's Regulator.

Additionally, if the Cloud Provider desires to terminate any portion of the services which it provides to the financial

[89] 2023 Interagency Guidance, *supra* note 12, at 934, discussing "Default and Termination".
[90] *Id.*
[91] IaaS Vendors should also have an obligation to provide transition assistance to its customers that provide services to financial institutions; OSFI Guideline B-10, *supra* note 6, at § 2.3.5 and Appendix 2 at subsection (l); IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 2 and Topic 6.

institution for the financial institution's breach of the Service Agreement, the financial institution should consider limiting it to the scope of the financial institution's material breach (*i.e.*, not the entire service) along with a meaningful opportunity for the financial institution to cure any such breach and for service to be then restored.

Financial institutions may require that the Cloud Provider not have the right to withhold transition services even if there is a dispute regarding fees or if the financial institution breached certain provisions of the Service Agreement. Similarly, financial institutions may require that the Cloud Provider not have the right to prevent the financial institution from obtaining a complete copy of the Customer Data whenever desired. Some Service Agreements do, however, permit the Cloud Provider to prohibit the Customer from accessing the Customer Data during a dispute. From a regulatory compliance standpoint, the availability of transition services and access to Customer Data by the financial institution should be independent from the Cloud Provider's prerogative to pursue its remedies.

Although Regulators and financial institutions are focused on operational certainty, Cloud Providers are focused on serving their many customers and expect to retain the ability to suspend their services in limited circumstances to address emergencies, especially those relating to security risk. Therefore, Cloud Providers reasonably may need the ability to suspend or otherwise cease providing its services if there is an event affecting the Cloud Provider's services that requires emergency response measures, such as a Cybersecurity Event (a "**Crisis**"). The financial institution could potentially accommodate the Cloud Provider's concern under certain conditions. First, the Cloud Provider should consider giving the financial institution prompt written notice, including all material details of the Crisis, prior to any suspension. The suspension should be in the most limited manner possible under the circumstances (*e.g.*, for the minimum number of end user accounts necessary to address the Crisis). Second, if the Cloud Provider actually suspends its services, the Cloud Provider should nevertheless consider allowing the financial institution to access the suspended services in order to remove, copy and back up Customer Data unless the Cloud Provider has a compelling reason to believe that permitting such access will cause a security risk to the services. During the suspension, the Cloud Provider should endeavor to promptly restore the suspended services and prevent future Crises by remediating the cause. Lastly, the Cloud Provider should aim to provide updates to the financial institution relating to the investigation and resolution of the events giving rise to the Crisis,[92] as well as details of remediation efforts implemented to prevent similar events. If the Cloud Provider is unable or unwilling to restore the services within an appropriate timeframe, the financial institution should have the right to terminate the Service Agreement or limit its use of the Cloud Provider to those portions of the services not impacted by the Crisis.

### M. Limitation of Liability

Not only do Regulators expect financial institutions to carefully assess the risks associated with the Cloud Provider's failure to perform under the Service Agreement, but Regulators also expect that the Service Agreement will

[92] FFIEC BCM, *supra* note 8, at § IV(A)(5), "Third-Party Service Providers."

appropriately allocate the financial risk between the parties.[93]

The financial institution should consider the Cloud Provider's creditworthiness and determine whether type and limits on the Cloud Provider's liability are in proportion with the risk of possible losses, including those caused by Cloud Provider to the financial institution or those that might prevent the Cloud Provider from fulfilling its obligations to the financial institution, and the activities performed. Accordingly, the Service Agreement should clearly set out: (i) the Cloud Provider's obligations and also the financial institution's responsibilities; (ii) the liability limits on the Cloud Provider, if any, for damages to the financial institution arising from the Cloud Provider's failure to perform its obligations under the Service Agreement; and (iii) the Cloud Provider's obligation to maintain types and amounts of insurance, notify the financial institution of material changes to coverage and provide evidence of coverage, as appropriate.

The limitation of liability provision is one of the most critical provisions in the Service Agreement. Key protections, such as indemnification, security and confidentiality obligations can be rendered largely illusory by limitations of liability that reduce the Cloud Provider's liability to a relatively trivial amount of damages. This is one of the most substantial areas of difficulty in negotiating almost any Service Agreement.

Cloud Providers typically attempt to disclaim or cap damages for their liability under the Service Agreement, generally at a dollar amount or as determined by formulae, often tied in some way to the amount of annual contract fees. Financial institutions are expected to assess whether any limits of liability are in proportion to the amount of loss the financial institution might experience as a result of a Cloud Provider's failures. Cloud Providers should consider to contractually agree to be liable for certain higher risk categories of damages, such as breach of privacy, information security and confidentiality, in an amount that is proportionate to the loss the financial institution may face as a result of such breach. Those actions could result in regulatory fines and costs associated with increased, prolonged or more frequent regulatory scrutiny or investigation(s) of the financial institution, hiring public relations firms, hiring forensic investigators or data recovery firms, mailing breach or data unavailability/corruption notifications, providing credit monitoring and call center services and defending against litigation.

Similarly, financial institutions expect that the Cloud Providers will agree to meet certain service levels[94] for its services and be willing to provide service level credits for failing to meet them. Such service level credits should be of the sort that sufficiently incentivizes Cloud Provider to comply with the service levels. The longer the initial term of the Service Agreement (*e.g.*, greater than three years, autorenewal provisions), the greater the need for specific, strong performance obligations and warranties. Service level credits should not be the financial institution's sole financial remedy if the service level failure causes damages beyond the amount of the service level credit. In any

[93] 2023 Interagency Guidance, *supra* note 12, at 933, discussing "Indemnification and Limitations on Liability"; OSFI expects a FRFI's Service Agreement to require vendors to "obtain and maintain appropriate insurance" and "notify the FRFI in the event of significant changes in insurance coverage." OSFI Guideline B-10, *supra* note 6, at Appendix 2 subsection (m).
[94] OSFI Guideline B-10, *supra* note 6, at Appendix 2 subsection (e); IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 1.

event, the financial institution's right to terminate the Service Agreement and seek recovery for repeated or egregious failure to meet agreed upon service levels should be expressly stated in the Service Agreement.

### N. Indemnification

Regulators expect financial institutions to carefully consider the parties' obligations to indemnify one another for certain third party claims, in light of the use case at hand and the associated risks to the financial institution, customers or other stakeholders.[95] Financial institutions expect that the Service Agreement should include, at a minimum, an obligation for the Cloud Provider to defend and settle third-party claims and hold the financial institution harmless from claims resulting from its material failure to perform its obligations, including any breach of privacy, confidentiality or information security obligations and failure to have and obtain the necessary intellectual property rights to provide the IaaS Services. The Service Agreement may also include the right for the financial institution to terminate the Service Agreement and receive a refund of prepaid, unused fees or release from monetary commitment if the Cloud Provider is unable to either provide a non-infringing and equivalent service or secure rights to continue providing its service.

Financial institutions should consider including in the Service Agreement provisions setting out the Cloud Provider's indemnity responsibilities for its negligence, gross negligence or violations of law in providing its services, as well as language to ensure that the financial institution is not held responsible for the Cloud Provider's negligence, gross negligence or violations of law. Beyond accepting negligence liability for insurable risks such as personal injury or damage to tangible property, financial institutions should expect that Cloud Providers will resist unlimited indemnification liability for negligent performance of the services and may instead consider robust service level agreement terms (see above).

Financial institutions should carefully assess indemnification clauses that require the financial institution to indemnify, defend or hold a Cloud Provider harmless from liability. Provisions requiring a financial institution to indemnify the Cloud Provider for claims that result merely from the financial institution's use of the Cloud Provider's services — but with no wrongdoing on the part of the financial institution — are rarely acceptable, as are requirements that the financial institution provide indemnification for the Cloud Provider's gross negligence, willful misconduct or breach of its obligations in the Service Agreement. In any event, any indemnification obligations imposed on the financial institution should only apply to claims asserted against the Cloud Provider by unaffiliated third parties and should allow the financial institution to have prompt notice of such claims, sole control of the defense or settlement and the right to reasonable assistance from the Cloud Provider in that defense or settlement.

### O. Unilateral Changes by Vendors

Service Agreements are often the product of extensive negotiations by the parties that culminate in contractual

[95] 2023 Interagency Guidance, *supra* note 12, at 933, discussing "Indemnification and Limitations on Liability".

compromises and acknowledgments of certain regulatory requirements. Therefore, if a Cloud Provider has the right to unilaterally change any aspect of the arrangement (including how the services work, service levels or how Customer Data is accessed or processed), it could undermine the parties' effort in negotiating the Service Agreement, as well as present significant challenges to the financial institutions in their management of their regulatory obligations. At a minimum, the Cloud Provider should be contractually prohibited from making changes to the terms of the Service Agreement or its services if such change is likely to result in a degradation of the features or security of the service or otherwise adversely impact the financial institutions rights, protections or benefits under the Service Agreement.

As discussed earlier in this paper, Regulators require financial institutions to perform appropriate due diligence and ongoing monitoring of Cloud Providers, including periodic review of the Service Agreement.[96] The type and level of risks may change over the lifetime of the Cloud Provider's relationship and financial institutions may adjust their ongoing monitoring practices accordingly, including changes to the frequency or type of information the financial institution requires from the Cloud Provider for such purpose. Therefore, financial institutions may seek to require all changes to the arrangement to be set forth in a written amendment to the Service Agreement. In some cases, however, Cloud Providers will seek the right to make unilateral changes on short notice, or no notice (*e.g.*, contract may incorporate hyperlink to the Cloud Provider's website terms). In other cases, Cloud Providers will offer a longer notice period (*e.g.*, for deprecating key services). As an alternative to the Cloud Providers' approaches, financial institutions may seek to: (i) limit the types of changes Cloud Providers may make unilaterally (often with an express contractual requirement that any Cloud Provider's changes will not result in a degradation of the features and security of the services); (ii) lengthen the notice period; (iii) require prior testing and approval by the financial institution; and (iv) reserve the right to terminate, without penalty, any services affected by the proposed changes.

## 4. Conclusion

While each financial institution and Cloud Provider will ultimately determine the contractual methodologies that best suits their own needs in the context of a Service Agreement, this paper has sought to elucidate the applicable regulatory requirements and guidance in the United States, the European Union, the United Kingdom and Canada, as well as suggest potential approaches to address a number of key contractual and regulatory considerations, including: subcontracting, audit, information and data security, security breaches and remediation, business continuity, confidentiality, retention of Books and Records, Customer Data controls, termination, non-renewal and suspension, limitation of liability, indemnification and the ability of vendors to make unilateral changes to services and terms.

[96] FFIEC Handbook, *supra* note 8, at 4 (highlighting due diligence and ongoing monitoring of service providers as key processes in effective risk management); OSFI Guideline B-10, *supra* note 6 at § 2.2.2; IIROC Outsourcing Guidance, *supra* note 6, at Appendix A Topic 1.

As discussed throughout this paper, there are often gaps between what financial institutions require and what Cloud Providers are willing to agree to contractually. Cloud Providers may object to certain regulatory requirements or financial institutions' contracting preferences based on the practical functionality of the particular Cloud Service or because of challenges in operationalizing such requirements or imposing them on existing subcontractors. While certain regulatory requirements are intractable, financial institutions may take a risk-based approach tailored to the use case to determine if and when certain requirements may be adjusted, or alternative solutions may be employed.

As the financial services industry continues to expand its use of cloud technology, we can expect the applicable regulatory and guidance landscape to evolve in response to changes in the technology and its use.[97] Both the financial institutions procuring these services and the Cloud Providers supplying them should remain mindful and vigilant in monitoring the regulations and guidance applicable to these relationships and in developing Service Agreements that balance Cloud Providers' concerns with financial institutions' need to comply with an increasingly broad and complex web of global regulations.

[97] *See* FFIEC Joint Statement, *supra* note 7, at 8-9, discussing various additional controls unique to cloud computing services, such as use of containers and managed security services in cloud computing environments.