sifma

Navigating Regulatory Challenges in Cloud Infrastructure Services Agreements

October 2020

BLG
Bortstein Legal Group

Contents

SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over $2.9 trillion for businesses and municipalities in the U.S., serving clients with over $20 trillion in assets and managing more than $72 trillion in assets for individual and institutional clients including mutual funds and retirement plans. 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 http://www.sifma.org.

Bortstein Legal Group (BLG), 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. BLG's extensive knowledge of global laws and regulations impacting financial institutions' use of technology, data and services allows BLG to help its clients ensure that their activities and contracts comply with evolving global standards. For more information, visit https://blegalgroup.com/.

Introduction

Financial institutions adopt innovative technology to provide better client service, improve operational efficiency, enhance compliance, and save money. Cloud technology may help financial institutions reach these goals. Many financial institutions want to expand their use sof cloud technology primarily for faster and cheaper scalability of computing power and data storage than is currently offered by more traditional, locally installed solutions. To date, many financial institutions have not expansively adopted cloud technology, partially due to the obstacles imposed by regulations and guidance and partially due to the industry's judiciousness in adopting new technologies. Nevertheless, financial institutions should address the increasingly critical position that cloud technology will occupy in their operations directly or indirectly.

Financial institutions should weigh the overall risks associated with having only a small number of vendors that provide Infrastructure as a Service services ("**IaaS Vendors**" and "**IaaS Services**"). The same IaaS Vendors provide IaaS Services directly to financial institutions as well as indirectly as subcontractors to many Software as a Service vendors ("**SaaS Vendors**"), Platform as a Service vendors ("**PaaS Vendors**") and other types of vendors (e.g., managed and professional service providers, consultants, law firms) that provide services to financial institutions (IaaS Vendors and all vendors that use IaaS Services to provide services to financial institutions are referred to as "**Vendors**"). Such widespread reliance on IaaS Vendors constitutes a concentration risk to financial institutions. To help mitigate concentration risks, and other risks associated with the failure or poor performance of IaaS Vendors, financial institutions could consider contractual obligations that support, and are consistent with, the applicable regulatory expectations and requirements.

SIFMA, in partnership with Bortstein Legal Group, developed this paper[1] to examine the general regulatory and guidance requirements in the United States, the European Union, the United Kingdom, and Canada,[2] applicable

[1] This paper is not intended to be a complete inventory and does not analyze every applicable global law and regulation.

[2] In Canada, the Office of the Superintendent of Financial Institutions Canada's [hereinafter OSFI's] Guideline B-10: Outsourcing of Business Activities, Functions and Processes, as supplemented by OSFI's Memorandum re New Technology-Based Outsourcing Arrangements dated February 29, 2012 [hereinafter OSFI Guideline B-10] guides outsourcing in the financial services sector by Canadian federally regulated entities (e.g. financial institutions such as banks and credit unions) [hereinafter Canadian FREs]. While Guideline B-10 is not strictly a regulation, it provides a set of expectations for prudent practices, procedures and standards to be included in material outsourcing arrangements, including expectations regarding risk management and contractual language. Canadian FREs determine such materiality in

Applicability to Regulated Vendors

Outsourcing and other vendor risk management regulations generally make no distinction between Vendors that Regulators have the authority to regulate ("**Regulated Vendors**") and those that Regulators do not have the authority to regulate. Therefore, Regulated Vendors tend to be subject to the same due diligence and on-going monitoring by financial institutions. However, Regulated Vendors, like financial institutions, may already be subject to annual audits, monitoring and the like by Regulators, evidence of which could be used to demonstrate compliance with certain regulatory requirements. At best this is done ad hoc as there is presently no Regulator attestation or certification that Regulated Vendors may readily provide to their financial institution clients.

to financial institutions' use of IaaS Services,[3] review the experience of financial institutions in attempting to address those expectations and requirements in their agreements for IaaS Services ("**IaaS Agreements**"), and consider some of the issues that the IaaS Vendors have raised in response to financial institutions' preferred contracting approaches, including how those requirements may conflict with IaaS Vendors' "shared responsibility" model and the capabilities of IaaS Services. In addition, this paper will identify contractual approaches that have been employed by IaaS Vendors and financial institutions to accommodate the IaaS Vendors' objections while satisfying the financial institutions' regulatory obligations.

Of note, the use of IaaS 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[4] and vendor concentration risk in order to mitigate reputational,

accordance with OSFI Guideline B-10 and, for such material outsourcing arrangements, will treat the OSFI Guideline B-10 requirements akin to regulatory requirements in order to meet OSFI's expectations.

[3] BLG's contributors to this paper include Larry Bortstein, Lou Trotta, Benjamin Ross, James Humphrey-Evans, Matt Johnson, David Cummings, Samantha Baer and Mike Tse. Additionally, Iain Duke-Richardet, Compliance Strategy Principal of Hearsay Systems (https://hearsaysystems.com/), made significant contributions to Section 8 (Books and Records). Iain is a recognized industry thought leader and subject matter expert on global technology-related legal and regulatory issues, including cybersecurity, privacy, communication and trading surveillance, books and records, and regulatory change management.

[4] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017); Office of the Comptroller of the Currency, OCC Bulletin No. 2013-29, Third-Party Relationships: Risk Management Guidance (2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html, at "Ongoing Monitoring" [hereinafter OCC Bulletin 2013-29]; Fed. Fin. Insts. Examination Council, Information Technology Examination Handbook, Outsourcing Technology Services Booklet (2004), *available at*

operational, security, financial and legal/regulatory risks associated with any such use.

Financial institutions and their Vendors, of course, will each decide for themselves whether or to what extent they adopt any of the suggestions set forth in this paper or incorporate in their respective agreements the considerations described herein based on their individual circumstances, including their business needs and due diligence protocols. Accordingly, nothing in this paper is intended to impose any contractual, legal or other obligations on any participant or suggest any agreement to the contrary.

1. Regulatory Expectations and Requirements

To minimize the risks associated with outsourcing, including with regard to financial institutions' use of Vendors, financial regulators ("**Regulators**") require[5] financial institutions to enter into written agreements with Vendors ("**Service Agreements**") and perform appropriate due diligence and ongoing monitoring of Vendors and their subcontractors, including via audit.[6] Regulators require the Service Agreements to require Vendors to extend contractual obligations, including audit rights, down to their subcontractors and to remain fully liable for the acts and omissions of their subcontractors;[7] and, in order for financial institutions to fulfill their due diligence and

https://ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf, at 18 [hereinafter FFIEC Handbook]; Fed. Fin. Insts. Examination Council Bus. Continuity Mgmt., *available at* https://ithandbook.ffiec.gov/media/274725/ffiec_itbooklet_businesscontinuityplanning.pdf, at Section IV(A)(5), "Third-Party Service Providers" [hereinafter FFIEC BCM]; Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk, December 5, 2013, *available at* http:// www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf, at Section IV [hereinafter Fed Guidance]; OSFI Guideline B-10 s.7.1 and s.7.3, the latter of which expects Canadian FREs to monitor Vendors and their significant subcontractors.

[5] *See supra* note 1.

[6] *Supra* note 4; OCC Bulletin 2013-29, *supra* note 4 at "Reliance on Subcontractors." The Office of the Comptroller of the Currency's ("OCC") examination procedures for evaluating the risk management of third-party relationships by national banks and federal savings incorporates an assessment of whether the examined entity has adequately conducted due diligence to verify whether the vendor counterparty or its subcontractors have publicly known outstanding issues with regulatory bodies or law enforcement. Office of the Comptroller of the Currency, OCC Bulletin No. 2017-7, Supplemental Examination Procedures for Risk Management of Third-Party Relationships (2017), https://www.occ.gov/news-issuances/bulletins/2017/pub-third-party-exam-supplemental-procedures.pdf at 6 [hereinafter OCC Bulletin 2017-7]; OSFI Guideline B-10 s.7.1, s.7.2.1(h) & s.7.2.1(i), the latter of which expects Canadian FREs to obtain the right in a Services Agreement to audit a Vendor's significant, rather than all, subcontractors. In addition, OSFI expects Canadian FREs to include in Service Agreements various clauses regarding Vendor performance, including the clauses covering the following: (a) performance measures to allow the Canadian FRE to determine whether Vendor's commitments are being fulfilled; and (b) the type and frequency of information the Canadian FRE receives from the Vendor, including performance measure reports. OSFI Guideline B-10 s.7.2.1(b) & s.7.2.1(c).

[7] Fed Guidance, *supra* note 4 at Section IV(C); FFIEC Handbook, *supra* note 4 at 14; OCC Bulletin 2013-29, *supra* note 4 at "Subcontracting"; OSFI Guideline B-10 *supra* note 4 and *supra* note 6. Regarding subcontracting, OSFI does not expect Vendors to be fully liable for the acts and omissions of their subcontractors (though Canadian FREs will often seek such protection), but does expect the following Service Agreement requirements to be flowed-down to subcontractors: the Vendor's confidentiality and data security obligations (for all

ongoing monitoring obligations, Vendors are also expected to, among other things, have subcontractors provide compliance and performance information to financial institutions.[8]

In addition, Regulators expect Vendors and their subcontractors to have comprehensive information security,[9] and business continuity and disaster recovery program,[10] requirements under their Service Agreements. This includes policies and procedures to ensure the confidentiality, security, integrity, and availability of the data of financial institutions and their clients, employees and others ("**Customer Data**") and the Vendors' and their subcontractors' systems.[11] Regulators also expect Service Agreements to include specific provisions relating to the Vendors' and their subcontractors' administrative, technical, organizational, and physical controls to safeguard Customer Data and their systems against unauthorized access, use, disclosure, modification, unavailability, and deletion.[12] Lastly, Regulators expect the Service Agreements to require the Vendors and their subcontractors to operate and maintain their services in accordance with the requirements of the laws, regulations, and regulatory guidance applicable to financial institutions.[13]

---

subcontractors), the Canadian FRE's audit and inspection rights (for significant subcontractors), and the Canadian FRE's monitoring rights (for significant subcontractors).

[8] OCC Bulletin 2013-29, *supra* note 4 at "The Right to Audit and Require Remediation" and "Subcontracting"; OSFI Guideline B-10, *supra* note 6.

[9] FFIEC Handbook, *supra* note 4; OCC Bulletin 2017-7, *supra* note 6 at 13; Fed Guidance, *supra* note 4; OSFI Guideline B-10 s.7.2.1(f) & s.7.2.1(j).

[10] OSFI Guideline B-10 s.7.2.1(g) & s.7.2.3, with respect to Vendors and not (expressly) subcontractors.

[11] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2017); Fed Guidance, *supra* note 4 at 6; OCC Bulletin 2017-7, *supra* note 6 at 13; OSFI Guideline B-10 s.7.2.1(j) which contains more general confidentiality and security requirements, but does specifically expect (a) that the Vendor's security and confidentiality policies be "commensurate with those of the [Canadian] FRE and at least be "reasonable" under the circumstances; and (b) the Vendor "to be able to logically isolate the [Canadian] FRE's data, records, and items in process from those of other clients at all times, even under adverse conditions."

[12] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2017); FFEIC Handbook, *supra* note 4 at 12; OSFI Guideline B-10, *supra* note 11. In addition, OSFI expects the Service Agreement to "detail the physical location whether the [Vendor] will provide the services." This expectation is often a difficult one for Vendors since serviced customer data in transit could be in multiple locations. OSFI Guideline B-10 s.7.2.1(a).

[13] FFIEC Handbook, *supra* note 4 at 15; OCC Bulletin 2017-7, *supra* note 6 at 13. Regarding Canada, this is not a specific requirement, but Canadian FREs will often attempt to obtain such covenants.

2. Shared Responsibility

Under the shared responsibility model, IaaS Vendors are responsible for providing the IaaS Services, including security for the equipment and facilities used to provide the IaaS Services and offering customers the features, functionality, and tools to configure the IaaS Services in a manner that meets their regulatory obligations, including security, data location, and other controls. Where an IaaS Vendor provides IaaS Services directly to a financial institution, the financial institution is responsible for understanding the use case (e.g., criticality of availability, type of data) and properly using the features, functionality and tools made available by the IaaS Vendor that are appropriate for that use case. The IaaS Vendor, however, should strongly consider including in the IaaS Agreement an obligation under which it will agree to provide and maintain the features, functionality and tools necessary to comply with requirements for all use cases and ensuring that they work properly.

Where an IaaS Vendor provides IaaS Services indirectly to a financial institution as a subcontractor (e.g., by hosting the infrastructure of other Vendors that directly provide services to a financial institution), the financial institution is responsible for understanding the use case. Those primary Vendors, however, are responsible for properly using the features, functionality and tools made available to them by the IaaS Vendors that are appropriate for that use case. In addition, the primary Vendors should strongly consider having agreements with IaaS Vendors that commit the IaaS Vendors to providing the features, functionality and tools and ensuring that they work properly to ensure that those other Vendors will be able to meet their obligations in a manner that satisfies the requirements of the financial institution.

3. Subcontracting

Regulators require financial institutions to perform appropriate due diligence and ongoing monitoring of subcontractors used by Vendors,[14] including in the context of outsourcing of a critical or important operational function.[15] Regulators also expect Vendors to remain fully liable for the acts and omissions of their subcontractors

[14] Fed Guidance, *supra* note 4 at Section IV(C); OCC Bulletin 2013-29, *supra* note 4 at "Ongoing Monitoring"; OSFI Guideline B-10, *supra* note 7.

[15] Telecom providers and the like are generally not considered sub-outsourcers for these purposes, notwithstanding the fact that the performance of the Vendor may rely on such providers. The Markets in Financial Instruments Directive ("MiFID") excludes the following from the scope of its general outsourcing requirements: the provision to the firm of advisory services, and other services which do not form part of

and maintain written appropriate agreements with all subcontractors.[16] Those agreements should protect the financial institution at least as much as the Service Agreement provides (including obligations relating to audit, security, confidentiality, privacy, compliance, business continuity and disaster recovery).[17] In addition, Regulators require financial institutions to maintain additional controls regarding a Vendor's use of subcontractors whose failure to perform has a material impact on the Vendor's performance or on the financial institution's use of the services ("**Material Subcontractors**").[18] Financial institutions therefore expect the Vendor to obtain the financial institution's written approval prior to using a Material Subcontractor in order to restrict the Vendor from delegating its obligations without the financial institution's prior written approval.[19]

---

the investment business of the firm, including the provision of legal advice to the firm, the training of personnel of the firm, billing services and the security of the firm's premises and personnel, and the purchase of standardized services, including market information services and the provision of price feeds. 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]; The European Banking Authority's ("EBA") Guidelines on Outsourcing Arrangement exclude the following from the scope of its outsourcing regulations: a function that is legally required to be performed by a service provider (e.g., statutory audit); market information services (e.g., provision of data by Bloomberg, Moody's etc.); global network infrastructure services (e.g., Visa, MasterCard); clearing and settlement arrangements between clearing houses, central counterparties, settlement institutions and their members; global financial messaging infrastructures that are subject to oversight by relevant authorities; correspondence banking services; and the acquisition of services that would otherwise not be undertaken by the institution or payment institution (e.g., advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g., plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g., electricity, gas, water, telephone line). EBA Guidelines on Outsourcing Arrangements (2019), at c. 4, Title 11, § 3, para. 38, *available at* https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf [hereinafter EBA Outsourcing].

[16] *See* FFIEC Handbook, *supra* note 4 at 14; OSFI Guideline B-10, *supra* note 7.

[17] Fed Guidance, *supra* note 4 at Section IV(C); OCC Bulletin 2017-7, *supra* note 6 at 13; OSFI Guideline B-10, *supra* note 7.

[18] Examples of Material Subcontractors could include subcontractors that (i) are dedicated to performance of the IaaS Services to the financial institution; (ii) perform a material aspect of the IaaS Services (e.g., the subcontractor manages the data center the IaaS Vendor uses to provide the IaaS Services to the financial institution); (iii) access, store or process (A) unencrypted Customer Data or (B) encrypted Customer Data that the IaaS Vendor has the means to decrypt (e.g., controls encryption keys); and/or (iv) communicate with any client of the financial institution or its affiliates. The EBA refers to "sub-outsourcing data", much like the concepts of chains of processors under European and United Kingdom data protection laws, as well as "sub-outsourcing of a critical or important function, or material parts thereof". EBA Outsourcing, *supra* note 12. Article 16(5) of MiFID provides that investment firms "shall ensure, when relying on a third party for the performance of operational functions which are critical for the provision of continuous and satisfactory service to clients and the performance of investment activities on a continuous and satisfactory basis, that it takes reasonable steps to avoid undue additional operational risk. Outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of its internal control and the ability of the supervisor to monitor the firm's compliance with all obligations." MiFID, *supra* note 12 at c. I, § 16(5*)*; OSFI Guideline B-10, *supra* note 7 & note 10. Further, as part of OSFI Guideline B-10's expectations, the Canadian FRE (x) should be notified in the event that the Vendor encounters circumstances that might have a serious impact on the service; and (y) should advise OSFI relationship manager about any events that are "likely to have a significant negative impact on the delivery of the service."

[19] FFIEC Handbook, *supra* note 4 at 14; OCC Bulletin 2017-7, *supra* note 6 at 13.

Financial institutions should conduct appropriate advance due diligence on each subcontractor used by the IaaS Vendor for each IaaS Service. Merely relying on already-completed due diligence may not satisfy financial institutions' regulatory obligations if the IaaS Vendor has a diverse suite of IaaS Services and uses different subcontractors to perform portions of those IaaS Services. Also, a change to how the IaaS Service is used by the financial institution (e.g., critical versus non-critical, whether the IaaS service will process Personally Identifiable Information, Material Non-Public Information, or other sensitive data) may impact the due diligence the institution would be expected to perform. Financial institutions therefore expect IaaS Vendors to provide detailed information, as well as advance notice of any changes, to financial institutions about their subcontractors to allow financial institutions to satisfy both their due diligence and on-going monitoring obligations.[20]

IaaS Vendors may resist accepting some of the contractual obligations that Regulators expect financial institutions to have in place to meet regulatory obligations. For example, financial institutions recognize that it would be difficult for an IaaS Vendor to seek and obtain prior written approval for use of all subcontractors from all financial institutions that use the IaaS Services (directly or indirectly through Vendors) – the IaaS Vendor 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. Financial institutions, therefore, may decide to take a risk-based approach based upon the contemplated use case for the IaaS Services, which may include foregoing the right to pre-approve Material Subcontractors so long as the IaaS Vendor makes the necessary commitments to satisfy the financial institutions' requirements for the use case. This may include, at a minimum, obligations for the IaaS Vendor to provide significant advance notice of the intention to use a Material Subcontractor and helping the financial institution to conduct the necessary due diligence on the new Material Subcontractor.[21]

While this approach may also satisfy the requirements of data protection laws in Europe and the United Kingdom, these requirements apply to any subcontractor which processes personal data on behalf of the financial institution

[20] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017); OCC Bulletin No. 2013-29, *supra* note 4 at "Ongoing Monitoring;" FFIEC Handbook, *supra* note 4 at 18; FFIEC BCM, *supra* note 4 at Section IV(A)(5), "Third-Party Service Providers;" Fed Guidance, *supra* note 4 at Section IV.

[21] OCC Bulletin 2013-29, *supra* note 4.

and there is no materiality qualification. This approach, however, is challenging for the financial institution in many circumstances (e.g., where the financial institution has made a substantial investment in transitioning to the IaaS Services or where termination and transition to a replacement Vendor or an in-house solution may require a protracted period to complete).

Moreover, the introduction of new Material Subcontractors may also raise complex compliance issues, including when those subcontractors are located outside the country of the financial institution, which would require cross-border transmission of regulated data.

4. Audit

A. Regulator Audit Rights

Regulators explicitly require the unfettered and unconditional right to conduct on-site audits of Vendors' (and their subcontractors') premises, data centers and systems in order to verify and ensure compliance with the Services Agreement and applicable laws and regulations (e.g., no restrictions or limits on access to certain locations or records or access to staff and 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).[22] Vendors (and their subcontractors) must also cooperate with Regulators and, at minimum, provide information requested by Regulators in connection with the provision of services to financial institutions (see "Books and Records" below).[23]

[22] Paragraph 87(a) of the EBA Guidelines states 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. EBA Outsourcing, *supra* note 15 at c. 4, § 13.3, para. 87; OSFI Guideline B-10, *infra* note 23. *See also*, MiFID *infra* note 25 and OCC Bulletin 2013-29 at "OCC Supervision" (discussing the Regulator's right to "examination oversight" with respect to third party service providers, "including access to all work papers, drafts, and other materials" and the Regulator's authority to "examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises").

[23] 17 C.F.R. § 240.17a-1 (2019); OSFI Guideline B-10, *supra* note 6. OSFI expects to do the following regarding audits with respect to the Vendor and significant subcontractors: (i) exercise the contractual audit rights of the Canadian FRE (of which OSFI expects, at a minimum, that the Canadian FRE or its independent auditor be able to evaluate the services, including the Vendor's internal control environment); (ii) accompany the Canadian FRE when it exercises its contractual audit rights; (iii) access and make copies of internal audit reports (and associated working papers and recommendations) prepared by or for the Vendor regarding the services performed for the Canadian FRE; and (iv) access findings in the external audit of the Vendor (and associated working papers and recommendations) regarding the services performed for the Canadian FRE.

B. Financial Institution Audit Rights

Regulators expect financial institutions to have the right to audit Vendors' (and their subcontractors') premises, data centers and systems[24]in order to verify and ensure compliance with the Service Agreement and applicable laws and regulations. The scope of the audits may depend upon the contemplated use case of the financial institution and the financial institution may consider taking a risk-based approach to consider whether the audits should include cybersecurity programs, disaster recovery and business continuity plans, and the testing of such programs and plans. In addition, financial institutions expect Vendor (and their subcontractors) to provide information reasonably requested by the financial institution in connection with the provision of services to the financial institution (e.g., response and completion of security questionnaires).

IaaS Vendors specifically should also strongly consider providing supporting information to other Vendors and permitting those Vendors to demonstrate to financial institutions that their use and configuration of the IaaS Services (in connection with their provision of services to financial institutions) substantially conform to their commitments to financial institutions under their Services Agreement and are consistent with the best practices recommended by IaaS Vendors.

Although it may be challenging for IaaS Vendors to provide all customers with the right to conduct on-site inspections and audits on data centers and systems, the applicable financial regulations and guidance require financial institutions to have such rights apply to both the Vendors and their subcontractors. Resolving this conflict may promote broader adoption and use of IaaS Services for all or some use cases.

C. IaaS Vendor Self-Audit and Reports

Regulators expect financial institutions to ensure that Vendors and their subcontractors will perform self-audits on a regular basis and provide those audit reports to the financial institutions. [25] As a result, IaaS Vendors should

---

[24] *Supra* notes 22 and 23.

[25] FFIEC Handbook, *supra* note 4 at 13; OCC Bulletin 2013-29, *supra* note 4 at "The Right to Audit and Require Remediation;" OCC Bulletin 2017-7, *supra* note 6; FFIEC BCM, supra note 4 at Section VII(I), "Third-Party Service Provider Testing;" Fed Guidance, *supra* note 4 at Section IV(C). MiFID provides that "the investment firm, its auditors and the relevant competent authorities [should] have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with this article, and the competent authorities are able to exercise those rights of access." MiFID, *supra* note 15 at Art. 31, § 2(i). The EBA places more reliance on "third-party certifications and third-party or internal audit reports" but only subject

strongly consider retaining a reputable external auditor to conduct an annual audit pursuant to the then current audit standards (currently SSAE 18). Upon request, the financial institutions expect the IaaS Vendor to provide a copy of the resulting report, such as a SOC 2 Report and if the financial institution reasonably believes that the SOC 2 Report does not address requirements set out in the Services Agreement, the IaaS Vendor should include those requirements in the next audit and report.[26] In the event a report identifies a material non-compliance, the Service Agreement should include a specific time period for remediation and termination rights, without penalty, if the Vendor fails to resolve the issue within the time prescribed.[27]

5. Information Security and Cybersecurity of Customer Data

Regulators expect Service Agreements to impose comprehensive information security program requirements on Vendors.[28] This includes requiring Vendors to have policies and procedures to ensure the confidentiality, security, integrity, and availability of Customer Data and the Vendors' and their subcontractors' systems.[29] In addition, Regulators expect Service Agreements to include specific provisions relating to the Vendors' administrative, technical, organizational and physical controls to safeguard Customer Data and the Vendors' systems against unauthorized access, use, disclosure, modification, deletion and unavailability, including requiring Vendors to flow such provisions down to their subcontractors.[30] As a result, financial institutions look for IaaS Vendors willing to commit to these requirements, whether they are contracting directly with a financial institution or with another Vendor that provide services to financial institutions.

to various conditions, including that the financial institution retains the contractual right to perform individual audits for the outsourcing of critical or important functions. EBA Outsourcing, *supra* note 15 at § 13.3, para. 91; OSFI Guideline B-10, *supra* note 23.

[26] OCC Bulletin 2013-29, *supra* note 4 at "The Right to Audit and Require Remediation;" Fed Guidance, *supra* note 4 at Section IV(C); OSFI Guideline B-10, *supra* note 23.

[27] FFIEC Handbook, *supra* note 4 at 13; OCC Bulletin 2013-29, *supra* note 4 at "The Right to Audit and Require Remediation."

[28] FFIEC Handbook, *supra* note 4 at 26; OCC Bulletin 2017-7, *supra* note 6 at 13; Fed Guidance, *supra* note 4 at 6-7; OSFI Guideline B-10, *supra* note 11.

[29] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2017); Fed Guidance, *supra* note 4 at 6; OCC Bulletin 2017-7, *supra* note 6 at 13; OSFI Guideline B-10, *supra* note 11.

[30] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2017); FFEIC Handbook, *supra* note 4 at 12; OCC Bulletin 2017-7, *supra* note 6 at 13; OSFI Guideline B-10, *supra* note 11 & note 18.

Vendors commonly seek to satisfy these requirements by agreeing to maintain an environment and internal controls consistent with the Vendors' then-current SOC 2 Report and by including specific requirements in the Services Agreement. In the case of Vendors who rely on IaaS Vendors to provide services to the financial institution, those Vendors may commit to maintaining the environment and internal controls to the extent permissible by its own IaaS Vendor. Based on the contemplated use case and a risk-based analysis, financial institutions may consider seeking to include certain commitments by the Vendors in the Service Agreement, including, at a minimum, appropriate controls regarding Vendor personnel and subcontractors (especially those that may access Customer Data) and Vendor's systems and infrastructure.[31]

As the services provider to financial institutions and other Vendors, the IaaS Vendor should strongly consider being contractually responsible for all of the appropriate controls unless its services agreement with either financial institutions or the other Vendors expressly states otherwise. Where the services agreement expressly states that the IaaS Vendor is not responsible, the IaaS Vendor should strongly consider, nevertheless, to contractually agree to provide and maintain the features, functionality and tools that allow financial institutions and other Vendors to appropriately configure the IaaS Services in a manner that satisfies security, data location and other requirements. The IaaS Vendor should also strongly consider agreeing to provide ample notice and detailed information regarding any changes.[32] Financial institutions expect the IaaS Vendor to be liable and responsible for any failures in such features, functionality and tools.

For example, Vendors conduct regular penetration tests on their systems to validate that the systems are adapting to the latest threats.[33] Vendors should also strongly consider sharing such results (including of tests of its subcontractors' systems) and permitting financial institutions to conduct their own penetration testing.[34] Financial institutions may be willing to agree to certain conditions to conducting its own penetration testing so long

---

[31] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.12 (2017); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.14 (2017); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.15 (2017); FFIEC Handbook, *supra* note 4, at 18-22, 24 and 29; FFIEC BCM, *supra* note 4 at Section V, "Business Continuity Plan;" OCC Bulletin 2013-29, *supra* note 4 at "Qualifications, Backgrounds, and Reputations of Company Principals" and "Ongoing Monitoring;" OCC Bulletin 2017-7, *supra* note 4, at 13, 14-15; Fed. Guidance *supra* note 4 at 9-10.]

[32] FFIEC Handbook, *supra* note 4, at 13.

[33] *Id*.

[34] *Id*.

as those conditions are specifically set out in the Service Agreement and the Vendor agrees to provide ample notice of changes to allow the financial institution to assess the impact of changes. In the event any penetration tests reveal deficiencies, financial institutions expect the Vendor to commit to tracking and remedying such deficiencies within a prescribed time frame appropriate for the criticality of the deficiency.[35]

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

6. 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**").[36] To assist financial institutions to meet their regulatory obligations, if an IaaS Vendor learns or has reason to believe that there has been a Cybersecurity Event, financial institutions expect Vendors to provide notice of the Cybersecurity Event to the financial institution in a timeframe that allows the financial institution to comply with applicable laws and regulations. Such notice should be in writing (including to an email address approved by the financial institution) and should include all material details of the Cybersecurity Event. In addition, the Vendor should strongly consider committing to promptly contain, control, and remediate any Cybersecurity Event and provide updates to the financial institution, upon request, relating to the investigation and resolution of the Cybersecurity Event.

For Vendors that rely on IaaS Services to provide their services to financial institutions, any unauthorized access or use of the IaaS Services could constitute a Cybersecurity Event. Therefore, in the services agreement between

[35] *Id.*

[36] 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 4 at 13; OCC Bulletin OCC Bulletin 2017-7, *supra* note 6 at 13; *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 Section 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."

the IaaS Vendor and those other Vendors, the IaaS Vendor should strongly consider agreeing to provide prompt notice and detailed information regarding any Cybersecurity Event to assist those Vendors to meet their obligations to financial institutions.[37]

7. Business Continuity

Regulators require financial institutions to take steps to ensure business resilience.[38] When a financial institution engages a Vendor, Regulators expect that the financial institution will assess how the Vendor 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.[39]

Regulators expect financial institutions to enter into Service Agreements that impose comprehensive business continuity requirements on Vendors (including exit strategies, as more fully detailed in Section 10 (Termination, Non-Renewal and Suspension by IaaS Vendor), below).[40] This includes requiring Vendors to implement and maintain business continuity plans, to share these plans with the financial institution, and to establish and follow procedures for testing and updating these plans.[41] In addition, Regulators expect that Service Agreements include provisions permitting financial institutions to participate in Vendors' tests of their business continuity plans, to be

[37] OCC Bulletin 2005-13, *supra* note 36.

[38] Fed Guidance, *supra* note 4 at Section IV(C); OCC Bulletin 2013-29, *supra* note 3; OSFI Guideline B-10, *supra* note 10.

[39] *Id*; OCC Bulletin 2017-7, *supra* note 6 at 13; OSFI Guideline B-10, *supra* note 10. In addition, OSFI expects Canadian FREs to cover the following in Service Agreements: (a) Vendors should be obligated "to report events to the Canadian FRE that may have the potential to materially affect the delivery of the service; and (b) whether the Vendor "must continue providing the service during a dispute and the resolution period, as well as the jurisdiction and rules under which the dispute will be settled. Finally, a Service Agreement between a Vendor and a Canadian FRE should "not contain wording that precludes the service from being continued in a situation where [OSFI] takes control of the [Canadian] FRE, or where the [Canadian] FRE is in liquidation." OSFI Guideline B-10 s.7.2.1(c), s7.2.1(d) and s.7.2.1(e).

[40] FFIEC BCM, *supra* note 4 at Section IV(A)(5), "Third-Party Service Providers;" Fed Guidance, *supra* note 4 at Section IV(C); OCC Bulletin 2017-7, *supra* note 4 at 13; *id*. at Section IV(E); FFIEC Handbook, *supra* note 4 at 12 and 15; Federal Deposit Insurance Corporation, Guidance for Managing Third-Party Risk, *available at* https://www.fdic.gov/news/news/financial/2008/fil08044a.html at Section 3 [hereinafter FDIC Guidance]; OCC Bulletin 2013-29, *supra* note 4 at "Performance Measures or Benchmarks" and "Business Resumption and Continuity Plans."; OSFI Guideline B-10, *supra* note 39.

[41] FFIEC BCM, *supra* note at Section VII(I), "Third-Party Service Provider Testing"; OSFI Guideline B-10, *supra* note 39.

notified of the outcome of the tests, and to review the results of the tests.[42] Further, Regulators expect Vendors to remediate any issues discovered during these tests.

Vendors may sometimes resist the ability of financial institutions to participate in business continuity plan testing. Vendors may also 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. Regulators expect that financial institutions will use a risk-based approach to determine if a Vendor's business continuity contractual commitments are sufficient in light of the nature of the Vendor's service and the scope of the data provided to the Vendor. Gaps often exist between what financial institutions require and what Vendors are willing to agree to contractually.

With regard to Vendors that rely on IaaS Services to provide their services to financial institutions, financial institutions expect those Vendors to have an obligation to configure the IaaS Services in a manner that enables them to meet their business continuity obligations to the financial institutions.[43] That also means IaaS Vendors should have an obligation to provide and maintain the functionality to assist those Vendors to meet their business continuity obligations to financial institutions.

8. Confidentiality

Regulators expect financial institutions to include in their Service Agreements appropriate confidentiality obligations protecting financial institutions' confidential information.[44] The Service Agreement should, at a minimum, prohibit the Vendor from using or disclosing the financial institution's confidential information (which is

[42] *Id.* As part of OSFI Guideline B-10's contingency planning expectations, OSFI expects that a Vendor be obligated to provide a Canadian FRE with notice in the event that the Vendor "makes significant changes to its resumption and contingency plans, or encounters other circumstances that might have a serious impact on the service."

[43] FFIEC Handbook, *supra* note 4 at 14.

[44] *Id*. at 13; OCC Bulletin 2013-29, *supra* note 4 at "Confidentiality and Integrity;" OCC Bulletin 2017-7, *supra* note 4 at 13; OSFI Guideline B-10, *supra* note 11.

generally broadly defined), and require the Vendor to protect the confidential information with appropriate security measures and to notify the financial institution of any disclosure or misuse.[45]

Regulators expect that the confidentiality obligations cover all the financial institution's confidential information, regardless of whether it is processed and stored on the IaaS Services. 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 and any resulting derivatives and analytics). Although it is common to exclude certain types of information from the IaaS Vendor's confidentiality obligations (e.g., publicly available information, information already known by the IaaS Vendor), these exclusions generally do not apply to Customer Data.

Financial institutions may also obtain confidential information about the IaaS Vendor when receiving the IaaS Services. This may include information regarding how the IaaS Services work, including reports describing the IaaS Vendor's security measures and business continuity plans. While it is generally acceptable for the financial institution to undertake confidentiality obligations relating to the IaaS Vendor'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 IaaS Services, and obtain related reports. Therefore, the parties should consider including in Service Agreements express language permitting the financial institution to disclose certain aspects of the IaaS Vendor's confidential information, such as information necessary to satisfy client due-diligence requests.

[45] FFIEC Handbook, *supra* note 4 at 13; OCC Bulletin 2013-29, *supra* note 4 at "Confidentiality and Integrity;" OCC Bulletin 2017-7, *supra* note 6 at 13; Fed. Guidance, *supra* note 4 at Section IV(C); OSFI Guideline B-10, *supra* note 39.

9. Books and Records

Vendors may provide services that create, or electronically store, data which financial institutions must retain pursuant to regulation.[46] 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.[47] While U.S. record retention standards remain subject to a rulemaking petition by industry associations,[48] Vendors should be willing to facilitate financial institution compliance with existing regulatory requirements.[49] For example, broker-dealers are required to create certain Books and Records and 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. When leveraging Vendor services, financial institutions are required to conduct due diligence on the IaaS Services and provide Regulators with notification. The following are the types of considerations that financial institutions and Vendors should consider regarding Books and Records requirements.

A. 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.[50] As a result, financial institutions and Vendors should consider storing 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.

---

[46] 17 C.F.R. §§ 240.17a-3 and 240.17a-4(f)(3)(vii) (2019) (Requiring regulated entities to make certain records. Books and Records includes, 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.).

[47] *Id.*

[48] *See* Addendum to Petition for Rulemaking to Amend Exchange Act Rule 17a-4(f) (May 24, 2018), *available at* https://www.sifma.org/resources/submissions/petition-for-rulemaking-to-amend-exchange-act-rule-17a-4f-addendum/.

[49] OSFI Guideline B-10 s.7.2.2. Certain records of Canadian FREs must, by their federal financial institutions legislation (e.g., certain customer banking records), be maintained in Canada.

[50] 17 C.F.R § 240.17a-4(f)(3)(ii) (2019); OSFI Guideline B-10 s.7.2.2 & s.7.2.3. OSFI expects the Canadian FRE to ensure that the Canadian FRE has "in its possession, or can readily access", all records necessary to allow it to sustain operations, meet its statutory obligations, and provide all information…required for OSFI to meet its mandate, in the event the [Vendor] is unable to provide the service."

B. Duplication

Regulators require financial institutions to retain a duplicate copy of the Books and Records.[51] Financial institutions will seek Vendor solutions that have functionality which maintains synchronized Books and Records (typically in different locations), including the attending indexes. Concurrently, Vendors should strongly 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 Vendor 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.

C. Deletion and Termination

Broker-dealers are required to retain Books and Records for a minimum time period.[52] Vendors 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 deletion action rests with the Vendor, clear documentation and signoffs from the financial institution must be pre-determined.

In addition to ongoing regulatory requirements, Vendors 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 Vendor'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 Vendor should hold a copy of the Books and Records until the transfer is complete

[51] *Id.*

[52] 17 C.F.R. § 240.17a-4(a)-(e) (2019) (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.)

because deleting Books and Records for any reason, including due to non-payment, could potentially result in the Vendor incurring secondary liability, abetting the financial institution in a violation of its regulatory requirements.

D. Third Party Undertaking

Third parties that store Books and Records for broker-dealers must file a written undertaking regarding those Books and Records.[53] Specifically, Regulators may request access to the Books and Records and request copies of the Books and Records. Where the financial institution or a Vendor uses the Vendor's solution for a purpose that generates Books and Records that are required to be retained, Regulators may consider the IaaS Vendor to be such a third party subject to these requirements. Further, if a Regulator contacts the Vendor to request for access or copies of records, the Vendor should notify the financial institution.

Therefore, for financial institutions to comply with these regulations when implementing IaaS Services, the Service Agreement should include language mandating the IaaS Vendor to regularly disclose the timelines of its product development plan. Concurrently, IaaS Vendors should agree to disclose such timelines to its 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 an IaaS Vendor 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.

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

[53] 17 C.F.R. § 240.17a-4(i) (2019).

10. Customer Data Controls

Regulators require financial institutions to maintain appropriate controls with regard to Customer Data, including 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, and knowing who has access to it (including access to encryption keys).[54] As a baseline, therefore, Vendors should consider agreeing to state in the Service Agreement that the financial institution retains ownership of all Customer Data and ancillary data (including usage reports, tracing of users, etc.) and that the Customer Data may be used solely for purposes of rendering the services to the financial institution. Vendors should also strongly consider contractually agreeing to provide and maintain the features, functionality and tools that allow financial institutions to back up Customer Data and specify where Customer Data will be processed and stored.[55] Given the potential for differences in laws from country to country, functionality that only allow for controls at the continent or region level is generally insufficient for financial institutions.[56] In addition, financial institutions may require Vendors to agree to not relocate Customer Data from the specified location unless approved or directed by the financial institution.[57] In order for financial institutions to meet their ongoing monitoring obligations, Vendors should strongly consider, upon request, providing the then-current locations where Customer Data is presently stored or processed. Certain jurisdictions may require additional obligations and language to be added to Service Agreements.

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

---

[54] *See* FFIEC Handbook, *supra* note 4 at 16; FFIEC BCM, *supra* note 4 at Section IV(A); OSFI Guideline B-10 s.7.2.1(f) & s.7.2.1(j).

[55] FFIEC Handbook, *supra* note 4 at A-5.

[56] FFIEC Handbook, *supra* note 4 at C-5.

[57] *See* FFIEC Handbook, *supra* note 4 at 13.

With regard to Vendors that rely on IaaS Services to provide their services to financial institutions, financial institutions may require those Vendors to configure the IaaS Services in a manner that enables them to allow financial institutions to maintain appropriate controls with regard to Customer Data. As a result, IaaS Vendors should have an obligation to make available the functionality to assist those Vendors to meet their obligations to financial institutions.

Finally, financial institutions should be wary of Vendors requesting broad rights in "aggregated data" derived from performance of the services. In many instances, the definition of what it means to "aggregate" is either missing or poorly defined. If such rights are to be granted, a clear definition of what it means to aggregate should be provided (i.e., data is de-identified 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).

11. Termination, Non-Renewal and Suspension by IaaS Vendor

Operational certainty of the IaaS Services is paramount to financial institutions particularly when they are used in the operation of critical activities (e.g., significant and/or client-facing functions).[58] For services where availability of the IaaS Services and access to Customer Data are essential, financial institutions expect that the Vendor will not be able to quickly or easily terminate, suspend, or not renew the services it provides to the financial institution.

Regulators require financial institutions to include in Service Agreements termination and notification provisions that allow for the orderly transition of services to an in-house solution or to another third party.[59] That means in all cases, including when the Vendor desires to terminate or not renew any portion of the services it provides to the financial institution, the Vendor should be able to do so only on appropriate notice to the financial institution and with the following obligations:[60]

[58] OCC Bulletin 2013-29, *supra* note 4 at "Termination."

[59] Fed Guidance, *supra* note 4 at Section IV(C); OSFI Guideline B-10, *supra* note 39; OSFI Guideline B-10 7.2.1(e).

[60] IaaS Vendors should also have an obligation to provide transition assistance to its customers that provide services to financial institutions; OSFI Guideline B-10 7.2.1(e).

1. Provide transition assistance to the financial institution.
2. Provide for the appropriate and orderly return retrieval, destruction and/or deletion of Customer Data.
3. Provide the financial institution with continued access to and use of the IaaS Services on an "as is" basis for a reasonable period in order to ensure an orderly transition.

Additionally, if the Vendor desires to terminate any portion of the services it provides to the financial institution for the financial institution's breach, it should consider limiting it to the scope of the financial institution's material breach (i.e., not the entire service) and accompanied by a meaningful opportunity for the financial institution to cure any such breach. Nevertheless, financial institutions may require that the Vendor 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 Vendor 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 Vendor 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 to the financial institution is independent from the Vendor's prerogative to pursue its remedies.

Although Regulators are focused on operational certainty,[61] IaaS Vendors are focused on serving their many customers and expect to retain the ability to suspend the IaaS Services in limited circumstances to address emergencies, especially relating to security risk. Therefore, IaaS Vendors reasonably may need the ability to suspend or otherwise cease providing IaaS Services if there is an event affecting the IaaS Services that requires emergency response measures, such as a Cybersecurity Event (a "**Crisis**"). The financial institution could potentially accommodate the IaaS Vendor's concern under certain conditions. First, the IaaS Vendor should strongly 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 IaaS Vendor actually suspends the IaaS Services, the IaaS Vendor should nevertheless strongly consider allowing the financial

[61] Fed Guidance, *supra* note 4 at Section IV(C).

institution to access the suspended IaaS Services in order to remove, copy, and back up Customer Data unless the IaaS Vendor has a compelling reason to believe that permitting such access will cause a security risk to the IaaS Services. During the suspension, the IaaS Vendor should endeavor to promptly restore the suspended IaaS Services and prevent future similar crises by remediating the cause. Lastly, the IaaS Vendor should aim to provide updates to the financial institution relating to the investigation and resolution of the events giving rise to the Crisis,[62] as well as remediation efforts implemented to prevent similar events. If the IaaS Vendor is unable or unwilling to restore the IaaS Services within an appropriate timeframe, the financial institution should have the right to terminate the Service Agreement or limit its use of the IaaS Services to those portions of the IaaS Services not impacted by the Crisis.

12. Limitation of Liability

Regulators require financial institutions to carefully consider the risks associated with the IaaS Vendor's failure to perform under the Service Agreement and appropriately allocate the financial risk between the parties.[63] The financial institution should consider the Vendor's creditworthiness and insurance coverages and determine whether limits on the IaaS Vendor's liability are appropriate in light of the damages the financial institution could suffer as a result of the IaaS Vendor's failure to perform its obligations under the Service Agreement or to comply with applicable laws.[64] Therefore, the Service Agreement should clearly set out (1) the IaaS Vendor's obligations and also the financial institution's responsibilities and (2) the liability limits on the IaaS Vendor, if any, for damages to the financial institution arising from the IaaS Vendor's failure to perform its obligations under the Service Agreement.

The limitation of liability provision is one of the most critical protections in the Service Agreement. It incentivizes the Vendor to perform as required and provides the financial institution with an appropriate level of recovery should the Vendor fail to perform. Key protections, such as indemnification, security, and confidentiality

[62] FFIEC BCM, *supra* note 4 at Section IV(A)(5), "Third-Party Service Providers."

[63] Fed Guidance, *supra* note 4; OSFI Guideline B-10 s.7.2.1(j). In addition, OSFI expects a Canadian FRE's Service Agreement to require Vendors to "notify the [Canadian] FRE about significant changes in insurance coverage and disclose the general terms and conditions of the insurance coverage". OSFI Guideline B-10, s.7.2.1(l).

[64] OCC Bulletin 2013-29, *supra* note 4; FDIC Guidance, *supra* note 40.

obligations can be rendered largely illusory by limitations of liability that reduce the Vendor'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.

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, and as discussed earlier in this paper and as another example, financial institutions expect that the IaaS Vendor agree to meet certain service levels for the IaaS 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 incentivize the Vendor to comply with the service levels. Providing those 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 event, the financial institution's ability to terminate the Services Agreement for repeated or egregious failure should be preserved.

13. Indemnification

Regulators expect financial institutions to carefully consider the parties' obligations to indemnify one another for certain third party claims.[65] Financial institutions expect that the Services Agreement should include, at a minimum, an obligation for the IaaS Vendor to defend and settle third party claims and hold the financial institution harmless from claims resulting from its failure to perform its obligations, including failure to have and obtain the necessary intellectual property rights to provide the IaaS Services. [66] Therefore, IaaS Vendors should provide a comprehensive indemnity in the event of a third party intellectual property claim and the Service Agreement should also include the right for the financial institution to terminate the Service Agreement and receive a refund of prepaid unused fees if the IaaS Vendor is unable to either provide a non-infringing and equivalent service or secure rights to continue providing the IaaS Service. Regulators expect that the Service Agreement set out the

[65] OCC Bulletin 2013-29, *supra* note 4; FDIC Guidance, *supra* note 40; Fed Guidance, *supra* note 4.

[66] Note that the Federal Reserve Bank states that "[i]ndemnification provisions should require the service provider to hold the financial institution harmless from liability for the negligence of the service provider" and "[l]egal counsel should review these provisions to ensure the institution will not be held liable for claims arising as a result of the negligence of the service provider." FFIEC Handbook, *supra* note 4 at page 15.

IaaS Vendor's responsibilities for its negligence in providing the IaaS Services and include language to ensure that the financial institution is not held responsible for the IaaS Vendor's negligence.

Regulators also expect financial institutions to carefully assess indemnification clauses that require the financial institution to indemnify, defend, or hold IaaS Vendors harmless from liability. Regulators have commented that broad indemnification provisions in Service Agreements are not reasonable. This includes provisions requiring a financial institution to indemnify the IaaS Vendors for claims that result merely from the financial institution's use of the IaaS services – but with no wrongdoing on the part of the financial institution – or from the Vendor'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 allow the financial institution to have sole control of the defense and the Vendor should provide reasonable assistance in that defense.

14. Unilateral Changes by Vendors

Service Agreements are often the product of extensive negotiations by the parties that culminate in contractual compromises and acknowledgments of certain regulatory requirements. Therefore, if a Vendor 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 and also present significant challenges to the financial institutions in their management of their regulatory obligations.

As discussed earlier in this paper, Regulators require financial institutions to perform appropriate due diligence and ongoing monitoring of Vendors.[67] 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, Vendors will seek the right to make unilateral changes on short notice, or no notice, and in other cases, Vendors will offer a longer notice period (e.g., for deprecating key services). As an alternative to the Vendors' approaches, financial institutions may seek to limit the types of changes Vendors may make unilaterally, lengthen the notice period and reserve the right to terminate any services affected by the proposed changes.

[67] FFIEC Handbook, *supra* note 4 at 4 (highlighting due diligence and ongoing monitoring of service providers as key processes in effective risk management).

Conclusion

While each financial institution and IaaS Vendor will ultimately determine the contractual methodologies that best suit its own needs in the context of IaaS Agreements, this paper has sought to elucidate the applicable regulatory and guidance requirements in the United States, the European Union, the United Kingdom, and Canada and to 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.

Regulators expect Service Agreements to require IaaS Vendors and their subcontractors to operate and maintain IaaS Services in accordance with the requirements of the laws, regulations and regulatory guidance applicable to financial institutions.[68] To reduce the risks inherent in outsourcing services, including IaaS Services, Regulators require financial institutions to enter into Service Agreements and perform sufficient due diligence and ongoing monitoring of IaaS Vendors.[69] Regulators also expect Service Agreements to require Vendors to have comprehensive information security and business continuity and disaster recovery programs.[70] Vendors must maintain adequate policies and procedures to ensure the confidentiality, security, integrity, and availability of Customer Data.[71] Service Agreements need to specifically address Vendors' administrative, technical, organizational, and physical controls to safeguard Customer Data and their systems against unauthorized access, use, disclosure, modification, unavailability, and deletion.[72]

In addition, all of the Regulators' expectations discussed in the preceding paragraph also apply to the Vendors' subcontractors, including requiring subcontractors to provide compliance and performance information to financial

[68] *Supra*, note 13.

[69] *Supra* note 8.

[70] *Supra*, note 9.

[71] *Supra*, note 11.

[72] *Supra*, note 12.

institutions.[73] Accordingly, Service Agreements should obligate Vendors to ensure their subcontractors comply with all contractual obligations, including audit rights (both of the financial institution and of Regulators), and Vendors must remain fully liable for the acts and omissions of their subcontractors.[74]

As discussed throughout this paper, there are often gaps between what financial institutions require and what Vendors are willing to agree to contractually. IaaS Vendors may object to certain regulatory requirements or financial institutions' contracting preferences based on the practical functionality of the particular IaaS Service or because of challenges in operationalizing such requirements or imposing them upon existing subcontractors. While certain regulatory requirements are intractable, in these instances, financial institutions may consider taking a risk-based approach in light of 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, and in particular IaaS Services, we can expect the applicable regulatory and guidance landscape, as well as industry best practices, to evolve in response to changes in the technology and its use.[75] Both the financial institutions procuring these services and the IaaS Vendors supplying them should remain mindful and vigilant in monitoring the regulations and guidance applicable to these relationships and in developing Service Agreements that balance IaaS Vendors' concerns with financial institutions' need to comply with an increasingly broad and complex web of global regulations.

[73] *Supra* note 8.

[74] *Supra* note 7.

[75] *See* Fed. Fin. Insts. Examination Council, Joint Statement on Security in a Cloud Computing Environment (2020), *available at* https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf, 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.