RISK	FI NEED	PROPOSED MITIGANT	REGULATORY BASIS	ADDITIONAL COMMENTARY
Insufficient audit rights to support the development of mitigating risk controls. (Report, Section 1.1.1)	Direct access to all key facilities through an onsite or virtual audit.	Annual audit rights, which may include pooling audits with peers, provided there is an opportunity for follow-up, physical inspection	• FFIEC Outsourcing Technology – Audit (p.13) • FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(d) • FSB 2023 – Enhancing Third-Party Risk Management and Oversight • FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	The best case scenario for FIs is certainly the ability to perform independent, stand-alone audits of all onsite and virtual environments applicable to the services; however, given the large pool of clients, it's reasonable for a consortium or pooling approach to be the first option.
Insufficient audit rights to extend access to regulators directly or indirectly (Section 1.1.2)	Ability for regulators to conduct an onsite or virtual audit and access audit reports	Audit rights that allow both the FI and its regulators to review evidence related to the entire control framework operated by the CSP, including physical facilities	• FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(q), and E • FSB 2023 – Enhancing Third-Party Risk Management and Oversight	
Chain subcontractors pose resiliency, supply chain and concentration risks (Section 1.2.1)	Transparency and audit rights over (i) full supply chain of critical subcontractors; and (ii) location of critical subcontractors' facilities, IT services, data processing activities and resilience.	Notice (at least 180 days in advance) and ability to veto critical subcontractors	• FSB 2023 – Contracting with nth-party service providers (3.2.2, 3.5.1) • FRB/OCC/FDIC 2023 – Interagency Guidance – C(3)n • FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	The FSB provides guidance on identifying "critical" third-party services. While it does not offer a singular definition of "critical subcontractor", it emphasizes a risk-based approach, suggesting that services should be deemed critical based on their potential impact on a financial institution's operations and the broader financial system.
Critical security vulnerabilities can have broad impacts on security and resiliency of CSP environments (Section 1.3.1)	Transparency over vulnerabilities to enable development of mitigating risk controls.	CSPs should notify FIs within a defined time frame of discovery of vulnerabilities, provide an RCA, and outline remediation	• FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 5(e) • FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	The Report notes that CSPs should provide this right without requiring the customer to subscribe to additional services or incur costs to receive the information. This demonstrates the common commercial barriers CSPs put in place to their customers getting the benefit of full transparency.
Regulatory and legal obligations require that FIs know where their data is at all times, and have the ability to control such data (Section 1.3.2)	Transparency over data residency, and robust consent rights before data is moved, or used for new or different reasons than originally agreed by the parties.	Agreements should prohibit the CSP from data relocation or use without approval, including using the data to train or improve the services.	• FRB/OCC/FDIC 2023 – Interagency Guidance – C(3)(c), C(4) FSB 2023 – Contract data access, ownership and location (3.2.2) • FFIEC Cloud Statement (2020)	These rights are particularly important to scope out appropriately when it relates to using customer data to train AI models.
Inconsistent methodology for notification of service availability or security incidents, which inhibits the FI from planning for planning and implementing mitigating controls or responses (Section 1.4.1)	Timely notification of incidents, including the impact to the FI; performance of an RCA.	Provide all FIs with a consistent communication method for all incidents that offers proactive notification, clear and consistent reporting time frames that align with regulatory obligations.	• FRB/OCC/FDIC 2023 – C(3)(h), 225.303 • FFIEC Outsourcing Technology (p.13) FSB 2023 – Incident notification (3.3) • SEC Reg SCI • FFIEC Joint Statement (2020)	This requirement should be fulfilled irrespective of the customer's support tier or financial commitment.
FIs are unable to understand the interconnected risk between the CSP services and other elements of the FI's IT infrastructure (Section 1.4.2)	Comprehensive understanding of service dependencies in order to better understand architecture and address downstream impacts of dependent system failure.	Disclose detailed description of the primary service, and all secondary service dependencies in the applicable documentation, including evidence of service testing and resiliency exercises.	• FFIEC Outsourcing Technology (p.13) • FRB/OCC/FDIC 2023 – C(3)(i) • FSB 2023 – Critical service exit planning (3.7)	
Inability to adapt to service deprecation prior to implementation of change (Section 1.4.3)	Sufficient notice of deprecation to allow for development of a responsive plan, and deployment of mitigating controls.	Provide 18 – 24 month notice prior to effectuating a service deprecation; obligation to assist in transition.	• FFIEC Outsourcing Technology (p.13) • FRB/OCC/FDIC 2023 – C(3)(i) • FSB 2023 – Critical service exit planning (3.7)	Most CSPs reserve the right to change, modify or alter the services during the term. It is similarly as common for notice of such changes to be issued via RSS feeds or other non-specific channels that require constant customer monitoring. More defined notice processes would alleviate this burden.
Compound and opaque risks from indirect cloud exposure (i.e., exposure to CSP risk via the broader supplier base) (Section 1.4.4)	Transparency and oversight of FI suppliers' cloud security posture **via CSPs enabling control validation capabilities**.	CSPs should provide the capability for their customers to demonstrate their cloud security posture (as developed with the CSP) to the customers' clients.	• FSB 2023 – Enhancing Third-Party Risk Management and Oversight – 3.5.1) • SEC Reg SCI	This requirement suggests that CSPs should be willing to offer much of the transparency and control not only to FIs but to unregulated customers that may be offering services in an FI ecosystem, whereby such services also rely on the CSP for hosting.
Confusion over allocation of responsibility for critical operational elements, like security (Section 2.1.1)	Complete and informed view of responsibility allocation.	Provide matrix mapping CSP vs. FI duties as it relates to security, resiliency and operational effectiveness; with periodic updates if changes arise.	FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	Pillsbury's Global Sourcing and Technology Transactions Team specializes in assisting organizations developing integrated delivery models. Even if CSPs are unwilling to provide a matrix as part of the Agreement, organizations would benefit from developing their own internal mapping of shared responsibilities in its IT infrastructure.
Costly mechanisms for de-migration, and lack of transparency leading to inability to develop a responsible exit plan (Section 2.2.1)	Consistent methods for transferring data/applications post-termination.	No-fee exit when compliance drives migration; mapping of services and functionality to enable the development of exit plans; at least 24 months' notice prior to terminating a product or service (plus an obligation to assist in de-migration).	• FRB/OCC/FDIC 2023 – C(3)(P) • FSB 2023 – Exit support (3.7) • FFIEC Joint Statement (2020)	
Lack of sufficient information related to business continuity incidents leading to inability to develop incident management protocols (Section 3.1.1)	Transparency regarding business continuity incidents.	Provide actionable guidance about common incidents.	• FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 3(c) • FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.6.1, 3.6.3 • FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	
Service availability incidents or cyber events cannot be fully assessed and tested because there is no right to participate in resiliency or cyber exercises (Section 3.1.2)	Right to participate in testing exercises to enable FI and its regulators to understand potential issues.	Perform, at least annually, exercises simulating resilience issues and common failure scenarios; provide a guidebook for how to address common failure scenarios; and permit FI participation.	• FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 3(c) • FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.6.1, 3.6.3 • FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)	
Inability to evaluate when operating changes to services could affect the ability of the FI to use the Services (Section 5.1)	Consistent communication regarding version changes, API changes, security key changes, significant upgrades, and new feature roll-outs.	Notify FIs if service changes based on a defined set of criteria and timeframes.	FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(c)	CSPs should also provide this right without requiring the customer to subscribe to additional services or incur costs to receive the information.
Changes to service terms, which may occur at a CSP's discretion, impact the ability of FIs to use the service under certain regulations, and could require changes to customer-managed controls (Section 5.1.2)	Notification that does not require periodic manual review.	Notify FIs of service term changes or additions; storage of all previous versions of service terms.	FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – 3(c)	
Undue risk for IP infringement, breaches of confidentiality, privacy, regulatory violations and security breaches by the CSP (Section 5.1.3, 5.1.4)	(a) Indemnification by the CSP for claims arising as a result of CSP actions. (b) limitations of liability that enable sufficient recovery for risks.	(a) FIs should not agree to contractual clauses that would require them to indemnify the vendor for their own negligence (or worse). (b) Liability levels should be proportionate to foreseeable losses.	FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – J. Indemnification and Limits on Liability	Customer indemnity obligations should also include carve outs for claims caused by the CSP negligence.