CLOUD OUTSOURCING ISSUES AND CONSIDERATIONS
JULY 2024

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

American Bankers Association®

sifma
Invested in America

Table of Contents

Introduction

The U.S. Department of the Treasury ("Treasury") completed a report in February 2023, *The Financial Services Sector's Adoption of Cloud Services*[1] ("Treasury Cloud Report"), to explore how the use of cloud services may affect the financial services sector's operational resilience. The Treasury Cloud Report identified six primary challenges associated with financial institutions' (FIs) acceleration of cloud adoption and related oversight including:

1. Insufficient Transparency to Support Due Diligence and Monitoring by Financial Institutions
2. Gaps in Human Capital and Tools to Securely Deploy Cloud Services
3. Exposure To Potential Operational Incidents, Including from Incidents Originating at a CSP
4. Potential Impact of Market Concentration In Cloud Service Offerings on The Sector's Resilience
5. Dynamics In Contract Negotiation Given Market Concentration
6. International Landscape and Regulatory Fragmentation

FBIIC-FSSCC Cloud Workstreams

After publishing the Treasury Cloud Report, Treasury developed a roadmap for addressing the six primary challenges through several FBIIC[2]-led, FSSCC[3]-led and FBIIC-FSSCC jointly-led workstreams to develop potential solutions and mitigation strategies. Three FSSCC-led workstreams were created with the intent to develop collaborative solutions between FSSCC member firms and associations and cloud service providers (CSPs) to enable FIs to meet regulatory expectations and maintain resiliency when using cloud services more easily. The FSSCC-led workstreams were:

1. Cloud Profile Refinement and Adoption
2. Cloud Outsourcing Issues and Considerations
3. Improving Transparency and Monitoring of Cloud Services for Better "Security by Design/Default"

This paper reflects the work of the *Cloud Outsourcing Issues and Considerations* workstream ("the workstream"), which is comprised of experts from FSSCC member firms and associations. The objective of the workstream is to address challenges raised in the Treasury Cloud Report related to transparency, resource gaps, exposure to operational incidents originating at CSPs. To meet this objective, the workstream developed this paper to identify the key issues for Fis to consider when obtaining services from CSPs.

Workstream participants developed these key considerations based on current regulatory expectations and challenges that FIs face to ensure their contracts with CSPs include the most appropriate provisions. The key considerations paper should be used as a voluntary reference tool by FIs to appropriately address cybersecurity, resilience, and third party-due diligence expectations, and to help enable FIs meet regulatory requirements and expectations.

[1] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
[2] Financial and Banking Information Infrastructure Committee (FBIIC): Charged with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall.
[3] Financial Services Sector Coordinating Council (FSSCC): Partners with the public sector on policy issues concerning the resilience of the sector. Its 70+ members consist of financial trade associations, financial market utilities, and financial firms.

Additionally, the workstream shared a draft of the paper with four CSPs in late March 2024 – Amazon Web Services, Google Cloud, IBM, and Microsoft – to seek their input and convened two meetings in April to review the key findings of the paper and to request comments by late May 2024. The workstream considered the thoughtful comments from several CSPs and incorporated some of their feedback in this paper. Based on CSP feedback, the workstream understands the earnest desire of CSPs to enable firms to manage risk and have greater transparency concerning shared responsibility in configuring and use of cloud services. CSPs assert that a flexible, risk-based approach consistent with the shared responsibility model will enable greater adoption of cloud consistent with an FI's risk appetite. The FSSCC workstream seeks to educate FIs about best practices when it comes to CSP services. The FSSCC also wants to continue our engagement with CSPs in order to mitigate the specific challenges outlined in the US Treasury paper and this paper. By mitigating these risks and regulatory compliance challenges, FIs and CSPs can continue to innovate responsibly.

Next Steps

The workstream confirmed the challenges identified in the US Treasury Cloud Report. Further, the workstream concludes that financial institutions, especially medium and small-sized financial institutions, will continue to face regulatory compliance challenges with the uneven bargaining power and contract negotiation dynamics unless CSPs embrace these recommendations. The workstream seeks a sustainable path forward for FIs of all sizes to maintain the ability to innovate through leading edge technology while meeting regulatory requirements and expectations. Hence, the workstream will prioritize the following activities as next steps:

1. Encourage FIs to use this paper as a reference tool during the contract negotiation process with CSPs.
2. Continue to seek opportunities to collaborate with CSPs to agree on the minimum baseline security and resiliency requirements and expectations to be included in contracts with FIs, based on the considerations outlined in this paper. One example of this type of collaboration is to align to the vision of the U.S. National Cyber Strategy and leverage the recommendations of the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) to drive continued advancements.
3. Encourage the U.S. Federal Banking Agencies (FBAs) to include relevant information about CSP's adherence to regulatory expectations in their reports of examination that the FBAs provide upon request to banks with active contractual CSP relationships.
4. Encourage US Treasury and US financial regulators to continue efforts supporting collaboration and coordination on financial regulatory issues arising from cloud service providers across FBIIC member agencies, relevant standards and international policies at the G7, Financial Stability Board and international financial standard-setting bodies.

Background

Financial institutions (FIs) are turning to cloud services for several reasons, including for the ability to deliver scalable, innovative, and cost-effective solutions for clients that enable them to remain competitive and relevant in a fast-paced environment. As one of the most regulated critical infrastructure sectors, particularly in the areas of cybersecurity and resilience, the financial services sector recognizes the importance of ensuring continuing operations and of providing the most secure experience for customers. FIs are currently balancing the need to meet customer expectations in an increasingly digital world, while also meeting regulatory requirements and expectations related to, but

not limited, cybersecurity, operational resilience, and third-party risk management, all centered around maintaining the safety and soundness of the financial market.

Increased Regulatory Focus on Third-Party Risk Management

Regulatory authorities in the United States (U.S.), European Union (EU), United Kingdom (UK), and Canada, among others, have recently updated and enhanced regulatory requirements or guidance applicable to FIs on third-party risk management ("TPRM"). It is within this context that regulatory expectations and risk management practices for cloud services have come into sharp focus. While some nuance exists across TPRM regulations, they generally set similar expectations and approaches. This includes a focus on the intended outcomes, which are agnostic to the type of service or service provider and leaves the details of risk management to each FI to best reflect the nature of their organization and service usage.

Fundamental to TPRM regulations is the application of a proportionate, risk-based approach. This enables FIs to tailor due diligence and oversight processes based on the specific risks presented by a third-party arrangement, such as a cloud service, across the entire lifecycle of the third-party arrangement. This lifecycle generally comprises four stages:

1. **Procurement Planning:** FIs evaluate and consider risks related to the potential third-party arrangement before entering a formal third-party relationship, including FIs' risk assessment of the service characteristics to determine the level of initial and ongoing due diligence required for a third-party arrangement.
2. **Due Diligence and Contract Negotiation:** FIs establish baseline protections, performance levels and minimum agreed upon controls through contracts to manage risk over the life of the relationship. FIs conduct initial due diligence to assess adherence of minimum agreed upon controls by the third-party (e.g., a CSP).
3. **Monitoring and Managing Suppliers:** FIs monitor suppliers to assess adherence to agreed-upon controls and manage risks to promote ongoing effectiveness of the provided service throughout the lifecycle of the relationship.
4. **Relationship Termination:** FIs and CSPs execute the necessary steps to disengage from the relationship and support the FI exit strategy to minimize disruption to the FI's services or operations.

Regulatory Expectations for Provision of Cloud Services

As FIs plan to shift more critical services to the cloud rather than on-premise, regulatory authorities have updated regulatory expectations specific to cloud services that go beyond traditional third-party risk management (TPRM) requirements. Some authorities are creating new regimes which may include direct oversight of CSPs and their service arrangements with the financial sector. Adjacent areas of TPRM regulation and guidance articulate additional expectations regarding how an FI engages, manages, and oversees services provided by CSPs. This includes cybersecurity; cyber resilience and testing; technology risk management; and data privacy and security, among others. Additionally, FIs are expected to have access to enough information from a CSP to satisfy growing operational resilience requirements and guidance, such as the ability to map services, assess supply chain risks, including "nth" party use by third-parties, understand critical services and dependencies, and determine the potential impact from a disruption of third-party arrangements, including cloud services.

While regulatory authorities are generally supportive of FIs' cloud services adoption, key underlying risks and concerns have prompted calls for change or clarity in the FI-CSP engagement dynamic. These

concerns include, but are not limited to:

- Insufficient transparency from CSPs, including on software and resilience dependencies, supply chain risks, resilience capabilities and testing, and incident notification
- Shared responsibility model and a clearer allocation of roles and responsibilities
- Indirect exposure from FIs' service providers' usage of cloud services, i.e., CSPs as fourth-parties
- Operational incidents and notification
- Supply chain or subcontractor risk
- Concentration risks
- Robust audit and access rights
- Vendor lock-in and limited portability capabilities
- Identification and management of FIs' nth party dependencies at the individual FI

Contractual Challenges

As FIs remain ultimately accountable to all applicable legal and regulatory requirements, securing contractual rights with CSPs is critical to executing appropriate oversight.

FIs are expected to include cybersecurity and operational resilience-related provisions in contracts with third parties, including CSPs, to demonstrate to regulatory authorities that the FI complies with related requirements. However, CSPs maintain it is cumbersome to manage unique contract clause requests from FIs that have the time, resources and leverage to negotiate these modifications. CSPs argue that this puts them in an untenable situation. As a result, the ability for FIs to negotiate with CSPs often depends on the FIs' bargaining power. Per the Treasury Cloud Report "[…unbalanced contractual terms could limit individual FIs' ability to measure and mitigate risks from cloud services, which could result in unwarranted risk across the sector." Further, smaller- and medium-sized FIs seeking to harness the benefits of cloud solutions and address related risk management and oversight needs may find themselves at a disadvantage when negotiating with CSPs.

Key Considerations

The FSSCC working group on Cloud Outsourcing Issues and Considerations developed a set of key considerations for FIs to use during contract negotiation and due diligence activities with CSPs in order to manage key risks and address regulatory authority concerns.

The key considerations span across the following areas: audit; subcontracting; data and security; service level agreements; notification and reporting; business continuity; indemnities; liability; and termination and exit. The key considerations also highlight specific regulatory expectations by US financial regulators and guidance from the Financial Stability Board (FSB). This includes a mix of regulatory requirements, guidance and toolkits. The workstream packaged these together and labeled them as "relevant regulatory expectations"; while there are distinctions in how regulatory requirements, guidance and toolkits are applied by financial regulators as it relates to enforcement actions, these holistic expectations effectively form the basis of FIs' supervisory interactions.

1. Secure Ability to Conduct Appropriate Due Diligence and Monitoring Activities

1.1 Audit

1.1.1 FI Audit Rights

Risk Description

Without sufficient audit rights, FI customers are unable to obtain information from CSPs to

validate existing controls, evaluate potential risks associated with the use of cloud services and to support development of mitigating controls.

FIs require direct access to all key facilities through an onsite or virtual audit of the service provider, based on their required third-party controls related to the delivery of the services by the CSP.

Mitigation Recommendation

In addition to providing audit reports, CSPs should provide each of their FI customers direct access to all key facilities through an onsite or virtual audit and its material subcontractors on at least an annual basis.

The audit rights should allow the FI customer to review evidence related to the entire control framework operated by the CSP and include inspection of physical facilities.

Use of "pooled audits" in which a CSPs works with a consortium of FIs to complete may provide helpful information to FIs if properly scoped. However, FIs should reserve the right for follow-up from pooled audits to address risks that are specific to FIs.

Relevant Regulatory Expectations:

- *Federal Financial Institutions Examination Council (FFIEC) Outsourcing Technology – Audit (p.13) sets the baseline.* "The institution should include in the contract the types of audit reports it is entitled to receive (e.g., financial, internal control, and security reviews)."
- *Federal Reserve Board (FRB)/Office of the Comptroller of the Currency (OCC)/ Federal Deposit Insurance Corporation (FDIC) 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(d).* "Such contract provisions 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."
- *Financial Stability Board (FSB) 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities.* "As part of their toolkit to assess and negotiate contracts for third-party service relationships, financial institutions can consider the following…Financial institution's right to access, audit and obtain relevant information from the service provider, as appropriate including information on supply chain risk management, which can extend to financial authorities."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Appropriate due diligence and ongoing oversight and monitoring of cloud service providers' security. As with all other third-party relationships, security-related risks should be identified during planning, due diligence, and the selection of the cloud service provider. Management should implement appropriate risk management and control processes to mitigate identified risks once an agreement is in place. The process for risk identification and controls effectiveness may include testing or auditing, if possible, of security controls with the cloud service provider; however, some cloud service providers may seek to limit a financial institution's ability to perform their own security assessment due to potential performance impacts."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Oversight and monitoring of cloud service provider-managed controls. Management should evaluate and monitor the cloud service provider's technical, administrative, and physical security controls that support the financial institution's systems and information assets that reside in the cloud environment. Oversight and monitoring activities include requesting, receiving, and reviewing security and activity reports from the cloud service provider; reports of compliance with service level agreements; product validation reports; and reports of independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments) performed on the cloud computing services."

CRI Profile v2.0 Control Objectives

- EX.CN-01.01: Contracts with suppliers clearly detail the general terms, nature, and scope of the arrangement, to include the distribution of responsibilities between the parties; costs, compensation, reimbursements, incentives, and penalties; service level agreements, performance measures, and benchmarks; responsibilities for providing, receiving, and retaining information; recourse provisions; and the organization's rights to review,

monitor, and audit the supplier's activities.

1.1.2 Regulatory Audit Rights

Risk Description

Financial regulators may require the FI to secure the right for the regulator to audit the FI's suppliers, including CSPs, directly or indirectly. This can include the ability of the regulator to receive both audit reports and other relevant information directly from the CSP and the ability to conduct an onsite or virtual audit, in order to address third party oversight activities where the FI cannot provide the relevant information and it must come from the CSP.

These rights are in addition to the annual audit rights provided to the FIs for third party oversight purposes.

Mitigation Recommendation

In addition to providing audit reports, CSPs should provide each FI customer and its regulators direct access to all key facilities through an onsite or virtual audit and its material subcontractors on at least an annual basis.

The audit rights should allow the FI customer and its regulators to review evidence related to the entire control framework operated by the CSP and include inspection of physical facilities.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(q).* "For relevant third-party relationships, it is important for contracts to stipulate that the performance of activities by third parties for the banking organization is subject to regulatory examination and oversight, including appropriate retention of, and access to, all relevant documentation and other materials. This can help ensure that a third party is aware of its role and potential liability in its relationship with a banking organization."
- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – E. Supervisory Reviews.* "When circumstances warrant, an agency may use its legal authority to examine functions or operations that a third party performs on a banking organization's behalf. Such examinations may evaluate the third party's ability to fulfill its obligations in a safe and sound manner and comply with applicable laws and regulations, including those designed to protect customers and to provide fair access to financial services. The agencies may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe or unsound banking practices by the banking organization or its third party."
- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities.* "As part of their toolkit to assess and negotiate contracts for third-party service relationships, financial institutions can consider the following…Financial institution's right to access, audit and obtain relevant information from the service provider, as appropriate including information on supply chain risk management, which can extend to financial authorities."

1.2 Supply Chain Risk Management

1.2.1 Subcontracting

Risk Description

FIs require more transparency over CSP chain subcontractors to ensure resilience, supply chain risk management and identification of concentration. Particular transparency and oversight is recommended of subcontractors considered material or critical, i.e., who provide a material part of the contracted service and whose failure could create significant risks to the FI.

Mitigation Recommendation

CSPs should provide transparency over critical/material subcontractors and audit rights over: (i) the full supply chain of critical/material subcontracting; and (ii) the location of critical/material subcontractor facilities, IT services and data processing activities, and their resilience.

CSPs should provide FIs sufficient notice (minimum of 180 days) prior to the implementation of a critical/material subcontractor so that FIs (or CSP) can address and resolve any objection or other concerns with the proposed change in or utilization of subcontractor. If the FI's objection or other concerns cannot be resolved, FIs have the right to terminate the contract if the FI does not approve of the subcontractor.

Relevant Regulatory Expectations:

- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.2.2.* "As part of their toolkit to assess and negotiate contracts for third-party service relationships, financial institutions can consider the following…Conditions governing sub-contracting to nth-party service providers;" *3.5.1* "contracts between financial institutions and third-party service providers may cover whether the latter may sub-contract critical services (or parts thereof) and, if so, subject to which conditions."
- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)n. Subcontracting.* "Banking organization may want to address when and how the third party should notify the banking organization of its use or intent to use a subcontractor and whether specific subcontractors are prohibited by the banking organization...Where subcontracting is integral to the activity being performed for the banking organization, it is important to consider more detailed contractual obligations, such as reporting on the subcontractor's conformance with performance measures, periodic audit results, and compliance with laws and regulations."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data at contract termination, and restrictions on the geographic locations where the financial institution's data may reside."

CRI Profile v2.0 Control Objectives

- EX.CN-01.02: Contracts with suppliers address, as relevant to the product or service, the supplier's requirements for managing its own suppliers and partners (fourth parties) and the risks those fourth parties may pose to the third party and to the organization, to include fourth party due diligence, limitations on activities or geography, monitoring, notifications, liability and indemnifications, etc.
- EX.CN-01.03: Contracts with suppliers address, as relevant to the product or service, the implications of foreign-based third or fourth parties, to include the relevance of local laws and regulations, access to facilities and data, limitations on cross-border data transfer, and language and time zone management.
- EX.MM-01.05: The organization regularly assesses a critical third party's program and ability to manage its own suppliers and partners (fourth and nth parties) and the risks those fourth and nth parties may pose to the third party and to the organization (e.g., cybersecurity supply chain risk, concentration risk, reputation risk, foreign-party risk, etc.)
- EX.MM-01.06: The organization regularly reviews the foreign-based operations and activities of a critical third party, or its critical fourth parties, to confirm contract controls are maintained and compliance requirements are managed.

1.3 Data and Security

1.3.1 Critical Vulnerabilities

Risk Description

Critical security vulnerabilities can have broad impacts on security and resiliency of CSP environments.

Mitigation Recommendation

CSPs should notify FIs within a defined time frame of discovery of critical vulnerabilities and should provide root cause analysis and an outline of remediation actions to be taken by the CSP or FI in a proactive manner, without requiring the FI customer to subscribe to additional services or incur costs to receive the relevant information from the CSP.

Relevant Regulatory Guidance:

- *FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 5(e).* "The firm identifies potential risk transmission channels, concentrations, and vulnerabilities by analyzing the interconnections and interdependencies within and across its critical operations and core business lines considering third-party risks. The information that is obtained from these analyses informs the firm's tolerance for disruption."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Ongoing oversight and monitoring of a financial institution's cloud service providers are important to gain assurance that cloud computing services are being managed consistent with contractual requirements, and in a safe and sound manner. This oversight and monitoring can include evaluating independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments), and evaluating corrective actions to confirm that any adverse findings are appropriately addressed."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… When defining responsibilities, management should consider management of encryption keys, security monitoring, vulnerability scanning, system updates, patch management, independent audit requirements, as well as monitoring and oversight of these activities and define responsibility for these activities in the contract."

CRI Profile v2.0 Control Objectives:

- EX.CN-02.02: Minimum cybersecurity requirements for third-parties include requirements for incident and vulnerability notification, to include the types of events requiring notification, notification timeframes, and escalation protocols.
- ID.RA-08.01: The organization has established enterprise processes for soliciting, receiving and appropriately channeling vulnerability disclosures from:
    1) Public sources (e.g., customers and security researchers);
    2) Vulnerability sharing forums (e.g., FS-ISAC);
    3) Third-parties (e.g., cloud vendors); and
    4) Internal sources (e.g., development teams).

1.3.2 Data Location and Usage by CSPs

Risk Description

FIs must know where their data is at all times in a CSP's environment in order to meet regulatory and legal obligations. In addition, CSPs should not be able to move FI customer data to any location outside of the selected CSP region (or outside a selected jurisdiction) without approval from the FIs.

FIs must also be able to control the use of their data by the CSP for only disclosed and approved purposes and limit any secondary data use by the CSP (including the ability to prevent or opt out of any usage by the CSP to train or improve CSP services).

Mitigation Recommendation

CSPs should either inform FIs of or provide a methodology for FIs to select, specific locations for their workloads to run in, including the actual physical location of their data within a CSP region or similar logical construct specific to a certain geography.

CSPs must not be able to move FI customer data to another location without the FI's approval. CSPs must disclose any identifiable metadata or other information collected from the FI's use of the CSP services and must provide an opt out function where FI customer data cannot be used

to train or improve services beyond the metadata collection.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(4).* "Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, as part of ongoing monitoring… The third party's reliance on, exposure to, and use of subcontractors, the location of subcontractors (and any related data), and the third party's own risk management processes for monitoring subcontractors."
- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(c).* "It is important to consider contract provisions that specify the third party's obligation for retention and provision of timely, accurate, and comprehensive information to allow the banking organization to monitor risks and performance and to comply with applicable laws and regulations. Such provisions typically address:
  - The banking organization's ability to access its data in an appropriate and timely manner; and
  - Whether the third party is permitted to resell, assign, or permit access to customer data, or the banking organization's data, metadata, and systems, to other entities.
- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.2.2.* "As part of their toolkit to assess and negotiate contracts for third-party service relationships, financial institutions can consider the following… Ownership and transferability of data as well as policies and controls for data access including potential access by other clients."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data at contract termination, and restrictions on the geographic locations where the financial institution's data may reside."

CRI Profile v2.0 Control Objectives:

- GV.SC-01.02: The organization regularly assesses the risk of its ongoing use of third parties in aggregate, considering factors such as critical service dependencies, vendor concentration, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.
- ID.AM-08.06: Minimum cybersecurity requirements for third-parties cover the entire relationship lifecycle, from the acquisition of data through the return or destruction of data, to include limitations on data use, access, storage, and geographic location.
- EX.CN-01.02: Contracts with suppliers address, as relevant to the product or service, the supplier's requirements for managing its own suppliers and partners (fourth parties) and the risks those fourth parties may pose to the third party and to the organization, to include fourth party due diligence, limitations on activities or geography, monitoring, notifications, liability and indemnifications, etc.

1.4 Notification and Reporting

1.4.1 Notification of Service Availability and Security Incidents

Risk Description

CSPs do not provide a consistent methodology for notifying FI customers of service availability or security incidents. The method and delivery for the Root Cause Analysis (RCA) at the conclusion of the incident is not consistent, and in many cases is provided only with a specific level of paid support. This results in the inability of FIs to receive timely information during an incident and analyze the impact to their services.

In addition, without the RCA, FIs cannot plan accordingly for future incidents or adequately understand what controls they could have implemented to mitigate or lessen the impact of such an incident to their applications.

Mitigation Recommendation

CSPs should provide FIs with a communication method for all incidents, regardless of their financial commitment to a support plan.

Additionally, RCAs for any service availability incident should be proactively provided to all FIs within disclosure, notification and reporting timeframes and the CSPs should be available to discuss the RCA with FIs, if requested.

For CSP security incidents that have material FI impacts, there should be an agreed upon notification timeline consistent with the FI's regulatory obligations.

CSPs should provide historical outage information, when requested.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(h).* "Another important provision is one that specifies when and how the third party will disclose, in a timely manner, information security breaches or unauthorized intrusions. … Such provisions typically stipulate that the data intrusion notification to the banking organization include estimates of the effects on the banking organization and its customers and specify corrective action to be taken by the third party."
- *FFIEC Outsourcing Technology (p. 13).* "Institutions should require the service provider to fully disclose breaches in security resulting in unauthorized intrusions into the service provider that may materially affect the institution or its customers. The service provider should report to the institution when intrusions occur, the effect on the institution, and corrective action to respond to the intrusion, based on agreements between both parties."
- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.3*. "Financial institutions may require third-party service providers to have clearly defined processes for identifying, investigating, remediating and notifying the financial institution in a timely manner of incidents that impact the third-party service provider's ability to deliver agreed-upon services or other obligations…Specifying incident reporting obligations in contracts can be an important tool for financial institutions."
- *FRB/OCC/FDIC – Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers – 225.303.* "A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data at contract termination, and restrictions on the geographic locations where the financial institution's data may reside."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Incident response capabilities… Additionally, the service level agreement should identify specific activities for incident response and identify the cloud service provider's responsibilities in the event of an incident. When responding to an incident, management should recognize shared responsibilities and corresponding duties. Often, cloud service providers offer a variety of monitoring and alerting tools that can be leveraged by a financial institution and integrated into its incident response plans."
- Securities and Exchange Commission (SEC): FI's subject to SEC Regulation Systems Compliance and Integrity (SCI) are required to ensure CSPs that operate SCI systems on their behalf that allow the FI to meet the requirements for reporting SCI Events (i.e., disruptions, intrusions, and compliance events).

CRI Profile v2.0 Control Objectives:

- GV.RM-05.02: The organization establishes minimum requirements for its third- parties that include how the organizations will communicate and coordinate in times of emergency, including:
    1) Joint maintenance of contingency plans;
    2) Responsibilities for responding to incidents, including forensic investigations;

3) Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and
4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.

- EX.CN-02.02: Minimum cybersecurity requirements for third-parties include requirements for incident and vulnerability notification, to include the types of events requiring notification, notification timeframes, and escalation protocols

1.4.2 Service Dependencies

Risk Description

CSPs do not provide a complete list of all service dependencies for each service they provide to customers. This creates the inability of an FI to understand the interconnected risk between each service. This prevents an FI from understanding how their architecture should be designed to address service unavailability, how incident playbooks should be designed to understand the downstream impacts of one services outage impact on another, and how a customer gains transparency on how a CSP manages their internal resiliency program to address service unavailability. This limits operational resilience planning and improvement efforts by FIs.

Mitigation Recommendation

CSPs should develop a common model for disclosure to complement the overall resiliency design of each service.

CSPs should provide a detailed description of each primary service, including control and data plane design, service type design, and all secondary service dependencies in their published service documentation.

CSPs should provide evidence of service testing and resiliency exercises to FI customers. This evidence can include third-party assessments and certifications if they vigorously evaluate the reliability, security, and resilience of CSPs' services in order to meet FI customer requirements.

1.4.3 Service Deprecation

Risk Description

CSPs commonly have the right to deprecate a service after a notification period. In many cases it is 12 months or less. This creates a very short window for an FI customer to be able to determine the impact of the service deprecation and develop a plan to address any required changes. In addition, service deprecation could create such an impact that the FI has to make significant changes requiring months or years of development or migrate their workload to another CSP or back on premise.

Mitigation Recommendation

CSPs should provide a minimum of 18 months before a service is deprecated. In addition, CSPs should be required to assist FIs in addressing the service commissioning and implement any recommended changes to their applications.

A further consideration could be for a CSP to be required to provide an alternative service to the deprecated one that provides the same or even improved functionality.

Relevant Regulatory Expectations:

- *FFIEC Outsourcing Technology (p. 13) – Business Resumption and Contingency Plans. "*The contracts should outline the service provider's responsibility to test the plans regularly and provide the results to the institution. … The service provider should provide the institution a copy of the contingency plan that outlines the required operating procedures in the event of business disruption."
- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(i).* "As such, it is important for the contract to address the third party's responsibility for appropriate controls to support operational resilience of the services, such as protecting and storing programs, backing up datasets, addressing cybersecurity issues, and maintaining current and sound business resumption and business continuity plans."
- *FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 4(b).* "The firm establishes relationships with third parties through formal agreements. The firm's manages and monitors the performance of third parties against its service requirements and its tolerance for disruption."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data at contract termination, and restrictions on the geographic locations where the financial institution's data may reside."
- SEC: Reg. SCI applies requirements to certain entities ("SCI Entities") that operate systems ("SCI Systems") that directly support the six specific functions that are central to the functioning of the U.S. securities markets (i.e., trading, clearance and settlement, order routing, market data, market regulation, and market surveillance). Reg SCI requires SCI entities to manage and oversee certain third-party providers, including cloud service providers, of covered systems.

CRI Profile v2.0 Control Objectives:

- GV.OC-05.01: The organization identifies, assesses, and documents the key dependencies, interdependencies, and potential points of failure to support the delivery of critical services (e.g., systems, business processes, workforce, third parties, facilities, etc.)
- GV.OC-05.02: The organization has prioritized its external dependencies according to their criticality to the supported enterprise mission, business functions, and to the financial services sector.
- GV.OC-04.04: The organization prioritizes the resilience design, planning, testing, and monitoring of systems and other key internal and external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.

1.4.4 Indirect Cloud Exposure

Risk Description

Direct cloud service usage represents only a partial view of the aggregate exposure, dependencies, and potential risks an FI faces from CSPs. Indirect exposure from CSP usage by an FI's supplier base is equally important to consider; however, FIs have limited transparency into the fitness of suppliers' cloud security posture.

Point-in-time assessments, as part of scheduled assurance activities by an FI, are effective but leave FIs open to risk on an ongoing basis. Enhancing transparency and oversight of FI suppliers' cloud security posture, via CSPs enabling control validation capabilities, would help address an FI's aggregate risk from CSP usage.

CSPs do not currently provide such reporting capabilities for FIs, although similar arrangements are currently available for insurance purposes. Commitment from CSPs to establish such capabilities for FIs would be a meaningful step to address this risk area.

Mitigation Recommendation

Contingent on consent from an FI's supplier, CSPs should provide the capability for their tenants to demonstrate their cloud security posture to their FIs' customers. The design of this new reporting should balance quality and confidence in the reported information with ease of

adoption across suppliers.

The reported security information should go beyond simple attestations and could be based on agreed parameters, such as standard control frameworks. FIs and CSPs should also consider the manner of delivery and frequency of the reported information.

Relevant Regulatory Expectations:

- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.5.1.* "Third-party service relationships often involve indirect reliance on other entities in the third-party service provider's supply chain (nth-party service providers) for the delivery of services to financial institutions. This indirect reliance should not lessen the regulatory responsibilities and accountability of financial institutions. Third-party service providers may have appropriate processes in place to address supply chain risks that may impact their ability to deliver services in line with contractually-agreed service levels;" *3.5.4.* "Where this is the case, financial institutions may consider these overlapping dependency relationships in their risk management."
- *SEC: FIs subject to SEC Regulation Systems Compliance and Integrity (SCI) are required to ensure CSPs that operate indirect SCI systems on their behalf meet the requirements for reporting SCI Events (i.e., disruptions, intrusions and compliance events).*

CRI Profile v2.0 Control Objectives:

- GV.SC-01.02: The organization regularly assesses the risk of its ongoing use of third parties in aggregate, considering factors such as critical service dependencies, vendor concentration, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.

2. Establish Roles and Responsibilities (i.e., Shared Responsibility Model)

2.1 Roles and Responsibilities

2.1.1 Shared Responsibility Model and Control Mapping

Risk Description

The shared responsibility model between a CSP and an FI is a key element in managing the use of public cloud. It is critical for the safety and soundness of the financial services industry that each FI understand every control managed by the CSP and every control that must be implemented by the FI, in order to utilize each service offered by the CSP.

CSPs do not provide a consistent and complete set of data to address this risk, which creates inconsistencies in an FI's understanding of what controls they must implement to achieve a minimum baseline of security and operational effectiveness.

Mitigation Recommendation

CSPs should provide a matrix defining the shared responsibility model for their services against a common controls framework set forth by the Cyber Risk Institute (CRI) that includes both CSP and FI responsibilities, including recommended controls to be implemented by the FI to achieve a minimum baseline of security, resiliency, and operational effectiveness.

CSPs should update this document regularly and within a specific timeframe when a service is changed, or when a new service is delivered.

Relevant Regulatory Expectations:

- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "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."

- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020)*: "Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider. 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. When defining responsibilities, management should consider management of encryption keys, security monitoring, vulnerability scanning, system updates, patch management, independent audit requirements, as well as monitoring and oversight of these activities and define responsibility for these activities in the contract. Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data at contract termination, and restrictions on the geographic locations where the financial institution's data may reside."

CRI Profile v2.0 Control Objectives:

- GV.SC-02.01: The organization clearly defines, and includes in contractual agreements, the division of cybersecurity and technology risk management responsibilities between the organization and its third parties (e.g., a Shared Responsibilities Model).

2.2 Termination and Exit

2.2.1 Vendor Lock-In/Portability and Exit Planning/Termination Assistance

Risk Description

CSPs do not provide transitional services of consistent methods for transferring data or applications from one CSP to another, or back on-premise, in the event of a forced or planned exit.

Most hyperscale CSPs provide for some type of functionality – normally the use of specific services for data migration – but the maintenance of that service is not contractually mandated and there is a risk it could be deprecated, preventing the FI from effectively moving its data without significant effort.

Further, in the event of a new regulation where the CSP cannot meet the regulatory requirements, forcing the FI to migrate its workload out of its current CSP, it must pay for data egress charges to move its data to another location. This creates an undue cost burden on the FI that was caused by the CSPs decision to not meet a specific regulatory requirement that is mandatory for the FI, incurring significant additional spend to migrate the applications and data to maintain regulatory compliance.

CSPs also do not provide a mapping of their services and functionality to other CSPs' services, creating a burden for each FI to develop regulatorily required Exit Plans on its own without utilizing service mapping that would expedite the process.

Mitigation Recommendation

CSPs should provide a service or function to allow for seamless data migration from any CSP to an alternative location for the duration of the FI's contract term and for a reasonable transition period.

CSPs should also not charge an FI for any data migration that is caused by their decision not to comply with a regulatory requirement that forces the FI to move its workloads to an alternative

location.

CSPs should provide service by service mapping and portability to facilitate exit planning activities for FI customers. It is advisable to agree with the service provider on all aspects of termination assistance, including scope, services to be provided, timing, service levels, time period, and costs.

CSPs should be contractually obligated to provide a minimum of 24 months notice prior to deprecating an SLA or terminating a product or service. In addition, the CSP should have the obligation to provide assistance to migrate the FI to a new service or to exit from the CSP entirely where the need to move products or exit from the CSP resulted from the change in SLA, service, or regulatory environment.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(P).* "An effective contract stipulates what constitutes default, identifies remedies, allows opportunities to cure defaults, and establishes the circumstances and responsibilities for termination. Therefore, it is important to consider including contractual provisions that:
    - Provide termination and notification requirements with reasonable time frames to allow for the orderly transition of the activity, when desired or necessary, without prohibitive expense;
    - Provide for the timely return or destruction of the banking organization's data, information, and other resources;
    - Assign all costs and obligations associated with transition and termination; and
        - Provide termination and notification requirements with reasonable time frames to allow for the orderly transition of the activity, when desired or necessary, without prohibitive expense;
        - Provide for the timely return or destruction of the banking organization's data, information, and other resources;
        - Assign all costs and obligations associated with transition and termination; and
        - Enable the banking organization to terminate the relationship with reasonable notice and without penalty, if formally directed by the banking organization's primary federal banking regulator.

- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.7.* "Financial institutions may appropriately plan, execute and oversee an exit from a critical service relationship by ensuring that there are appropriate:
    - Contractually agreed transitional periods to minimise the risk of disruption;
    - Processes to ensure that, where applicable, the financial institutions' logical assets (e.g. data and applications) and physical assets are returned in a cost-effective and timely manner, and in a format that allows them to continue their business operations; and
    - Provisions relating to the ownership, maintenance, preservation, and long-term availability of records (including audit trails and other regulatory records).
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020):* Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider… . Management should also consider… expectations for removal and return of data at contract termination…"
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020):* "Consideration of interoperability and portability of data and services. When selecting or designing and building cloud computing services, management may consider interoperability and portability in the design of those services or application providers. A financial institution's interoperability and portability strategy will depend on the institution's risk appetite and the contracted service model (e.g., SaaS, PaaS, or IaaS) employed. Management may consider these capabilities as part of the initial contracting and design of cloud computing services."

CRI Profile v2.0 Control Objectives:

- EX.DD-01.01: Documented procurement plans are developed for initiatives involving elevated business, technical, or cybersecurity risk in order to establish criteria for the evaluation and selection of a supplier, and any special requirements for organizational preparation, supplier due diligence, and contract terms.

- EX.TR-01.01: The organization establishes contingencies to address circumstances that might put a vendor out of business or severely impact delivery of services to the organization, sector-critical systems, or the financial sector as a whole.

3. Ensure CSPs Provide Incident Management Playbooks and Participate in Business Continuity Testing and Resilience Exercises

3.1 Business Continuity

3.1.1 Business Continuity Planning: Incident Management Playbooks

Risk Description

CSPs do not provide consistent descriptions of common incidents that could occur in the use of their services in a manner that is easily consumed by FIs. This puts the burden on the FI to develop incident management protocols to address all failure models that could occur.

Mitigation Recommendation

CSPs should provide actionable guidance to customers about common incidents and best practices for their overall service environment and individual service usage. This would provide every FI customer a starting point to develop their own incident management program specific to their consumption of CSP services. The actionable guidance should be updated regularly for new incident types and new services as applicable.

CRI Profile v2.0 Control Objectives:

- GV.SC-08.01: The organization's resilience strategy, plans, tests, and exercises incorporate its external dependencies and critical business partners.
- EX.DD-03.02: The organization reviews and evaluates a prospective critical third party's business continuity program, to include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.
- EX.MM-02.02: A process is in place to confirm that the organization's critical third-party service providers maintain their business continuity programs, conduct regular resiliency testing, and participate in joint and/or bilateral recovery exercises and tests.

3.1.2 Business Continuity Testing and Resilience Exercises

Risk Description

CSPs participate inconsistently with resiliency or cyber exercises. This creates a risk that a service availability incident or cyber event that effects multiple customers, or an entire specific regional location where many customers run their workloads, cannot be fully assessed, and tested in a game day scenario where multiple customers and regulators can participate and understand the best practices to address the problem.

Mitigation Recommendation

CSPs should participate in relevant exercises and develop realistic scenarios that could occur in their service environment. This should be ongoing, occurring at least annually.

CSPs should also develop and publish, in coordination with the relevant FI industry groups and regulators, common failure scenarios (extreme but plausible) that could occur across the industry and how those scenarios could be mitigated by CSP or customer controls.

FIs would also encourage CSPs to participate in industry-wide exercises.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2020 – Sound Practices to Strengthen Operational Resilience – 3(c).* "The firm tests business continuity plans, reviews the execution of tests, and improves plans by incorporating lessons learned. Business continuity tests and exercises incorporate dependencies of critical operations and core business lines on third parties. When possible, the firm participates in disaster recovery and business continuity testing with third parties associated with critical operations and core business lines.
- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.6.1.* "Clear, up-to-date and appropriately tested business continuity planning to address the continuity of critical services is key to safeguarding the operational resilience of financial institutions. In particular, financial institutions may [seek] to ensure that their relationships with third-party service providers commit them to:
  - Implement appropriate business continuity plans (and other relevant plans such as contingency plans, disaster recovery plans and incident response plans) covering critical services they provide to the financial institution;
  - Regularly test these plans and share the results, including lessons learnt, vulnerabilities and remediation actions; and
  - Support the testing of financial institutions' business continuity plans as appropriate."
- *FSB 2023 – Enhancing Third-Party Risk management and Oversight: A toolkit for financial institutions and financial authorities – 3.6.3.* "Financial institutions may ensure that third-party service providers:
  - Develop and maintain business continuity plans informed by a comprehensive BIA, and set out clear, measurable indicators (e.g. RTOs, RPOs, maximum potential loss). Indicators used by third-party service providers could complement and support those used by financial institutions in their business continuity plans, in particular where financial authorities require financial institutions to meet specific RTOs;
  - Regularly test their business continuity plans and share relevant findings (including vulnerabilities), lessons learnt, and remediation actions planned or undertaken; and
  - Conduct joint business continuity testing with financial institutions (individually or collectively), where appropriate and feasible."
- *FFIEC Joint Statement on Security in a Cloud Computing Environment (2020): "*Business resilience and recovery capabilities. Operations moved to cloud computing environments should have resilience and recovery capabilities commensurate with the risk of the service or operation for the financial institution. Management should review and assess the resilience capabilities and service options available from the cloud service provider. There may be several configurations available, and management should determine which options best meet the institution's resilience and recovery requirements. Resilience and recovery capabilities are not necessarily included in cloud service offerings; therefore, the contract should outline the resilience and recovery capabilities required by the institution. Based on the cloud service model used, management should evaluate and determine how cloud-based operations affect both the business continuity plan and recovery testing plans. As with other operations, management should regularly update business continuity plans to reflect changes to configurations and operations and regularly test and validate resilience and recovery capabilities. Testing may need to be conducted jointly with the provider depending on the service model being used."

CRI Profile v2.0 Control Objectives

- ID.IM-02.08: The organization tests and exercises, independently and in coordination with other critical sector partners, its ability to support sector- wide resilience in the event of extreme financial stress or the instability of external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.

4. Explore How to Measure and Monitor the Potential Impact of Market Concentration In Cloud Service Offerings On The Sector's Resilience

The challenges raised by Treasury in this area are notable, but not the core focus of this workstream; however, the recommendations provided in this document, in addition to the outputs of related FSSCC cloud workstreams, would help mitigate certain risks inherent in concentrated cloud service offerings.

5. Improve the Ability of FIs to Negotiate Contracts with CSPs

5.1 Operational and Legal Changes to Services

Risk Description

CSPs do not consistently communicate when operating changes to services could affect the ability of the FI to utilize the services. Examples are version changes, application programming interface (API) changes, security key changes (secure ciphers and cryptographic standards), significant upgrades to a service, new feature rollouts, etc. Without this information, FIs cannot evaluate changes, nor can they take a change at CSP into account when a service incident occurs, and they are attempting to troubleshoot why a service is not operating as expected or is unavailable.

While it is acknowledged that all changes made to CSP services cannot be made in real time due to the nature and frequency, any change that could impact a FI's use should be communicated proactively to the FI to evaluate the impact.

Mitigation Recommendation

CSPs should notify FI customers if service changes based on a defined set of criteria and timeframes. Notification must be proactive and not require costs like enterprise support or other mechanisms that a customer must pay for to receive the notifications.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – C(3)(c).* "Notification to the banking organization of significant strategic or operational changes, such as mergers, acquisitions, divestitures, use of subcontractors, key personnel changes, or other business initiatives that could affect the activities involved."

CRI Profile v2.0 Control Objectives

- EX.MM-01.01: The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to manage and monitor its third-party relationships to a degree and extent commensurate with the risk each third party poses to the organization and the criticality of the third party's products, services, and/or relationship to the organization.
- EX.MM-01.04: The organization regularly assesses critical third party adherence to service level agreements, product specifications, performance metrics, resource level/skill commitments, and quality expectations; addresses performance issues; and exercises contract penalties or credits as warranted.

5.1.2 Ongoing Changes to Legal Services Terms

Risk Description

Most CSP contracts allow for the changes to individual service terms as part of the ongoing evolution of the service. These terms are usually listed on the CSP website, but no formal process of notifying an FI customer exists when the service term is changed, or a new service term is added. This puts the burden on the FI to create a program to manually review the service terms for changes and can create gaps in knowledge for service evaluation if the review is not conducted at regular intervals. Changes to service terms could impact the ability of the FI to use a service under various regulators, and/or require changes to customer managed controls in order to continue to use the service in line with internal or external regulatory requirements.

Mitigation Recommendation

CSPs should proactively notify FI customers when any individual service term changes, when new services are added to the service terms and store all previous version of service terms for access by the FI customer.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – 3(c).* "It is important to consider contract provisions that specify the third party's obligation for retention and provision of timely, accurate, and comprehensive information to allow the banking organization to monitor risks and performance and to comply with applicable laws and regulations. Such provisions typically address: Specification of the type and frequency of reports to be received from the third party, as appropriate. This may include performance reports, financial reports, security reports, and control assessments."

CRI Profile v2.0 Control Objectives

- EX.MM-01.01: The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to manage and monitor its third-party relationships to a degree and extent commensurate with the risk each third party poses to the organization and the criticality of the third party's products, services, and/or relationship to the organization.
- EX.MM-01.04: The organization regularly assesses critical third party adherence to service level agreements, product specifications, performance metrics, resource level/skill commitments, and quality expectations; addresses performance issues; and exercises contract penalties or credits as warranted.

5.1.3 Indemnities

Risk Description

Indemnification provisions should require the service provider to indemnify and hold the FI harmless from key risks such as intellectual property infringement, breaches of confidentiality and privacy, regulatory violations and security breaches. Legal 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.

Mitigation Recommendation

FIs should not agree to contractual clauses that would require them to indemnify the vendor for its own negligence (or worse).

5.1.4 Limitations of Liability

Risk Description

Some service provider standard contracts may contain clauses limiting the amount of liability that can be incurred by the service provider. If the institution is considering such a contract, management should assess whether the damage limitation bears an adequate relationship to the amount of loss the FI might reasonably experience as a result of the service provider's failure to perform its obligations.

Mitigation Recommendation

Agreements between FIs and CSPs should include liability levels proportionate to foreseeable losses.

Relevant Regulatory Expectations:

- *FRB/OCC/FDIC 2023 – Interagency Guidance on Third-Party Relationships: Risk Management – J. Indemnification and Limits on Liability*

- *"Incorporating indemnification provisions into a contract may reduce the potential for a banking organization to be held liable for claims and be reimbursed for damages arising from a third party's misconduct, including negligence and violations of laws and regulations. As such, it is important to consider whether indemnification clauses specify the extent to which the banking organization will be held liable for claims or be reimbursed for damages based on the failure of the third party or its subcontractor to perform, including failure of the third party to obtain any necessary intellectual property licenses. Such consideration typically includes an assessment of whether any limits on liability are in proportion to the amount of loss the banking organization might experience as a result of third-party failures, or whether indemnification clauses require the banking organization to hold the third party harmless from liability."*

6. Harmonize the Global Regulatory Landscape

The challenges raised by Treasury in this area are notable but not the core focus of this workstream; however, a common cross-border regulatory and supervisory approach to FI-CSP arrangements, including on contractual rights, could help address certain regulatory fragmentation challenges.