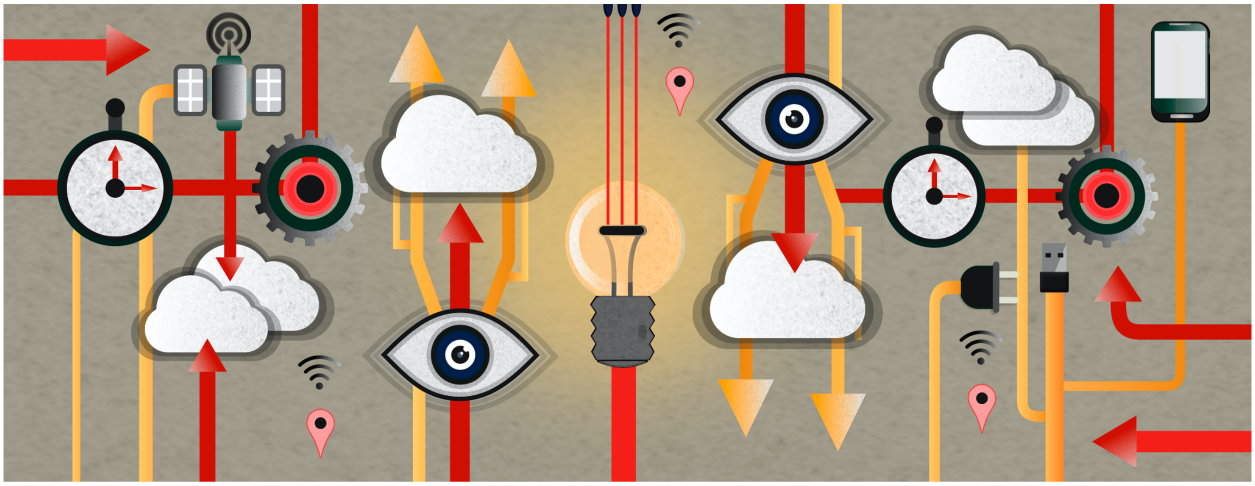

FSI MIGRATION TO GOOGLE CLOUD:

Key regulatory considerations in the United States

Prepared by Global Markets Advisory Group LLC

James Buckley, Louis Pastina, Charles Dolan, and Daniel Labovitz

March 2022

Table of Contents

Executive summary

Cloud computing continues to experience significant growth within the financial services sector for the beneficial solutions it offers in areas such as data security, increased processing capacity, and resilience. The increasing use by Financial Services Institutions (FSIs) of outsourced cloud services by providers such as Google Cloud have similarly resulted in an effort by US regulators to adapt their approach to reviewing such arrangements and providing guidance to FSIs considering using a public cloud. To a significant degree, the regulators' guidance outlines certain common themes, building on long-established principles governing risk management controls for any outsourced function. As FSIs continue to migrate mission-critical, computerized operations and controls from an on-premises data center to a public cloud, the importance of a comprehensive and well-documented risk assessment and governance process cannot be overstated.

FSIs considering moving operations to the cloud must assure that they will continue to comply with the applicable rules, regulations and guidance issued by the banking, securities and commodities regulators. The requirement of ongoing compliance must inform the project from the outset, and involve all necessary stakeholders within the FSI, including technology, operations, legal and compliance personnel, whose respective roles are further articulated in Appendix 3. Advancing a cloud migration strategy without assuring that potential issues have been identified and all relevant stakeholders have had the opportunity to provide timely input can result in delays in completing the migration, with potential impacts to operational planning and efficiency, as well as increased costs. Simply stated, executing on a successful cloud migration strategy requires a multi-disciplinary team with full knowledge of the scope of the project, who are empowered to raise potential issues of concern within their respective areas of responsibility.

The obligation for continuous and ongoing compliance also covers any FSI systems post-migration to a public cloud provider. Accordingly, strong governance controls on the parts of both the FSI and the Cloud Service Provider (CSP) are of critical importance.

This whitepaper is intended as a guide for FSIs to help them meet US regulators' expectations regarding both the initial process of migrating to Google Cloud and in the post-migration operating environment.

Regulatory considerations in moving FSI applications to Google Cloud

FSIs operating within the U.S. banking and capital market sectors are subject to an extensive regulatory structure designed to assure that all aspects of an FSI's operational and technological functions are compliant with the governing laws, rules and regulations to which they are subject. Each regulator has adopted rules and/or issued guidance regarding outsourcing arrangements, including those involving public cloud providers, and have outlined a risk-informed process.[1] There are commonalities across regulators in their approach and there are overarching considerations that will inform the decision by an FSI to migrate to the cloud.[2]

Regulators have identified the following critical areas of focus for FSIs to satisfy regulatory requirements:

- ☐ **Identifying areas of risk and implementing strong governance controls-** Developing and executing on a strong governance process covering critical areas such as (i) systems development, operations, and the documentation surrounding those functions; (ii) handling of system outages; (iii) maintaining data security; (iv) planning for business continuity and disaster recovery, and (v) fulfilling recordkeeping obligations applicable to FSIs.
- ☐ **Post-migration supervision and controls** – Key elements of a program of supervision and control include risk monitoring and system audits/reviews; review of controls around

[1] This report addresses common regulatory requirements that all the U.S. financial services regulators have promulgated through rules or in written guidance to FSIs under their regulatory jurisdiction.

[2] See Appendix 1 for a list of current regulatory requirements applicable to FSIs that impact migrating operations to the cloud.

system changes and the potential impact to hosted FSI systems and applications; and, clearly articulated communications processes/protocols between the FSI and the CSP. These factors are critical to an effective and ongoing program of supervision and control; moreover, these considerations have been identified by regulators as necessary elements of proper oversight of the performance of any third-party provider, including CSPs. Particular risk areas that should always be subject to ongoing supervision include:

(i) incident notification and response procedures, including an explanation of the incident and the remediation measures that may need to be reported by the FSI to regulators, both during the incident and upon its full remediation. The reporting obligation resides with the FSI as the regulated entity, but will likely require the CSP to provide information regarding the incident. Depending on the regulator, the timeframes for reporting incidents can be extremely short. The written supervisory policies and procedures of the FSI should address such reporting requirements, and the role of the CSP in assisting the FSI to report within required regulatory timeframes should be described in the contract;

(ii) business continuity and disaster recovery, (including any potential latencies that could impact services running in real time on cloud services);

(iii) cybersecurity with a strong focus on the division of responsibilities between the FSI and the CSP with respect to threat detection, incident response, and any required patching or updating;

(iv) physical security controls to assure that the CSP has adequate physical and environmental controls to safeguard its facilities, technology systems, and data.

(v) regular testing of FSI systems operating in the cloud. FSIs are required to perform testing of their operational systems to assure compliance with applicable regulatory requirements. A well-planned testing regimen is an integral part of a cloud migration process and FSIs must work collaboratively with the CSP to test system performance in the cloud environment. The FSI should document the results of these tests and retain related documentation (e.g., test scripts, test case results, quality assurance and user acceptance testing materials) as part of the FSI’s books and records. Regular testing post-migration is also necessary, especially where the FSI or the CSP make system changes or enhancements that could impact cloud-hosted applications or data.

- ☐ **Addressing regulators’ expectations** - FSIs must work collaboratively with the CSP to address regulators’ expectations regarding their cloud-hosted systems and respond to inquiries in a timely manner. This will entail having an agreed-upon process with the responsibilities of each party identified, both for any required notifications to regulators regarding system performance issues and for routine examinations. Depending on the circumstances, the FSI may need to communicate any system-related issues impacting the performance or compliance of its cloud-hosted systems to its regulators within a defined (and in some cases very short) timeframe. The protocols established between the FSI and the CSP for incident management and reporting should address this potentiality and provide for prompt notifications between the parties and a documented process for investigating, determining the root cause of the issue, timely reporting, and resolution.

Effective risk assessment and governance controls

The regulators in the banking, securities and commodities sectors have long recognized that FSIs can outsource key business, technology and regulatory compliance functions to third-party vendors, and the use of vendors to support critical FSI systems and operational processes has become widespread. Since an FSI always retains the responsibility for assuring that any function performed by a third-party vendor supports full compliance with all regulatory obligations, any such arrangement must be subject to a thorough risk assessment and governance process that assures the entity’s ongoing compliance and operational effectiveness, including in critical areas such as cybersecurity, data governance, business continuity and recordkeeping.

Regulators have stated that that the level of due diligence and oversight should be commensurate with the risk associated with the activity. An FSI’s management should have a clear understanding of the controls that the CSP is responsible for managing and those controls that the FSI is responsible for configuring and managing, and that understanding should be documented in the contract between the FSI and the CSP and in all service-level agreements (SLAs), including termination provisions that assure that the FSI will be able to access its data and other relevant information after its relationship with the CSP has ended. These documents are essential to articulating and delineating the respective roles and responsibilities between the CSP and FSI. Key elements of the required risk assessment are the CSP's business experience and qualifications; financial condition; legal and regulatory compliance; risk management and control processes; information security; and operational resilience.[3]

The risk management process outlined by regulators provides a template for an FSI to follow before determining to move any systems, applications or processes to the cloud. Program governance and a full vetting by all relevant stakeholders are critical to the process. In fact, one of the main impediments to a successful migration strategy is a failing to adopt a clearly articulated roadmap for implementation. While the initial decision to consider using the cloud may be driven by technology requirements, it should not be made solely by the FSI's senior level technologists (i.e., the Chief Technology Officer, the Chief Information Officer, or the Chief Information Security Officer). Involvement by all relevant stakeholders across the enterprise from inception is critical to assure that the decision to migrate to the cloud will not be impeded by legal, operational or regulatory considerations.[4]

Project and vendor management and systems testing

Given their reliance on computerized systems and the need to safeguard their data (e.g., relating to customers, transactions, and the institution's overall financial and operational "health"), FSIs must have effective project management and vendor management functions. The importance of a strong project management function in any cloud

[3] See Appendix 2.

[4] Appendix 3 contains a table that expands on the regulators' guidance shown in Appendix 2 and organizes tasks according to which key stakeholders may (depending on the organization) have a critical role in ensuring a successful migration to Google Cloud.

migration effort cannot be overstated, and it is critical to both its implementation and the post-migration operation of cloud-based systems.

As in other critical risk areas, an FSI’s approach to implementing and operating in the cloud should be clearly articulated in written policies and procedures that are reviewed regularly to assure that they are current. Regulatory inquiries and reviews can be expected to focus on appropriate governance and ongoing oversight in the pre- and post-implementation phases.[5]

A robust vendor management program is essential for FSIs to meet their continuing responsibility to oversee, supervise, and monitor a CSP’s performance. Regulators have encouraged FSIs to conduct testing of CSPs as part of their due diligence obligations, and FSIs should expect that regulators will likely want to review test plans, test performance, and the results of any follow-up.

To support its FSI customers in meeting the requirements described above, Google Cloud has committed to partnering with FSIs as they execute their internal risk management program requirements and their regulatory compliance controls. Google Cloud’s commitment to protecting the privacy of data stored by its FSI customers is summarized in the Google Cloud Trust Principles, and evidenced by its built-in data protection controls, including encryption in transit, encryption at rest, identity and access management, and in its approach to data deletion. These are a few examples to illustrate Google Cloud’s robust security and data privacy risk management posture.

Google has consistently provided thought leadership around these critical regulatory functions. Google Cloud has published whitepapers on topics ranging from security, architecture, data governance and the use of AI/ML, among others. Google Cloud’s

[5] CSPs are not subject to FSI regulators’ jurisdiction and therefore the regulators are generally not in a position to evaluate a CSP’s risk controls, including its project management processes for onboarding customers; additionally, a CSPs risk management protocols and processes can vary from those employed by an FSI . As a result, regulators continue to examine their approaches to reviewing these relationships which, in turn, provides an opportunity for both the regulated entities and CSPs to work collaboratively to assure that regulators understand, and can effectively examine, cloud-based systems and applications that support an FSI’s business.

approach to security, privacy and compliance controls has been independently verified via the successful completion of third party audits and globally recognized certifications, all of which are available for review and inspection.

Google's shared fate model

The security of the cloud and what is in it against intrusions and other threats is of critical importance to both the FSI and Google. Both parties have the responsibility to protect and promote cloud security. Google has focused on enhancing its partnership with its cloud customers for security infrastructure by moving to what it has described as the "shared fate model."

Google's shared fate model contrasts from the standard "shared responsibility model" in cloud computing, which governs the allocation of specific obligations between the CSP and the customer with respect to the security of, and data in, the cloud. When an FSI transitions from an on-premises data center to that of the CSP, responsibility for various controls is shared between them, with each party's responsibilities determined by the cloud computing service model being employed (i.e., the degree of the FSI's responsibilities vary depending on whether it is leveraging the cloud for IaaS, PaaS, or SaaS services). This differentiation of responsibility is sometimes referred to as security "**OF**" the cloud versus security "**IN**" the cloud.[6]

Google's shared fate model is a move to shift the dynamic, enabling customers to use cloud services as a platform for managing risk, rather than a risk to be managed. To this end, Google has developed tools and processes that "cross boundaries" between Google's systems and those of the customer. This will have the effect of bringing the governance and oversight that regulators expect of FSIs using an outsourced public

[6] Under the shared responsibility model, the CSP is responsible for the "Security **OF** the Cloud" meaning that it protects the infrastructure that runs all of the services (the hardware, software, networking, and facilities that it relies on to run its cloud services). The FSI customer in that situation is responsible for "Security **IN** the Cloud." The scope of the customer's responsibility will depend on the specific services it selects and any applications it chooses to migrate.

cloud, and Google’s own governance and oversight of its cloud platform, into closer alignment. Importantly, the model does not limit the customer’s accountability, including accountability to regulators.

Operating within Google Cloud

As stated above, after an FSI migrates to Google Cloud, it retains the responsibility to assure that its systems and applications continue to operate as designed and in compliance with all its regulatory obligations. Accordingly, regulatory guidance provides that FSI’s operating systems in the cloud must have strong governance and risk management programs to oversee their cloud-based operations. Many of these risk and governance activities are similar to, or continuations of, those undertaken during the risk-management assessment in preparation for migration to the cloud. Examples of such activities include the following:

- **Ongoing monitoring** – As noted above, regulators have stated that ongoing supervision and monitoring are essential components of third-party risk management, and the appropriate degree of ongoing monitoring is commensurate with the level of risk and the complexity of the third-party relationship (i.e., the higher the risk of the outsourced activity, the more comprehensive monitoring is appropriate). Elements of an effective ongoing monitoring program include, among other things, reviewing relevant audits and reports pertaining to the third-party provider, monitoring for compliance with applicable legal and regulatory requirements, and reviewing any changes by the cloud provider to its policies, procedures and controls. Regulators have also stated that FSIs should require cloud providers to make timely notifications of any material changes to its systems or processes utilized to perform an outsourced function.

FSIs must assure that they have adequate resources and qualified personnel to effectively perform ongoing monitoring and an escalation path to senior management of the FSI and its Board of Directors. FSIs should be diligent in assuring that the process for ongoing monitoring and documenting the results are part of the FSI's written policies and procedures. These policies and procedures should be regularly reviewed and updated as necessary.

- **Effective Controls** – As noted above, FSIs are expected to maintain effective vendor management programs, especially those that operate in or use third-party cloud services. With the increasing reliance on distributed technology, vendor management is essential to cybersecurity risk management.[7] Google is responsible for monitoring threats, responding to incidents and performing patches for vulnerabilities for its cloud services; but the FSI similarly has responsibilities for the security of the applications and processes it has programmed to operate in the cloud.[8] The security of the FSI's applications hosted in the cloud should be subject to periodic testing in coordination with the CSP and the results of these tests should be retained by the FSI as part of its books and records.

Addressing regulators' questions and concerns regarding an FSI's cloud migration

In summary, financial regulators in the U.S. have provided guidance to regulated entities on managing the risks associated with using a public cloud provider such as Google.

[7] For example, the SEC has identified three practices that it expects to see in strong cybersecurity programs: (i) establishing a vendor management program to ensure vendors meet security requirements established between the entity and the vendor, as well as the vendor's adherence to the practices it has undertaken; (ii) understanding the vendor relationship and how cloud-specific risk and security was to be addressed (e.g., how the shared responsibility is operationalized); and (ii) vendor monitoring and testing. *See* OCIE Cybersecurity and Resiliency Observations Report, p. 8 (Jan. 27, 2020).

[8] For any Google Cloud references, please refer to https://cloud.google.com/security/best-practices

Each regulator has stated unambiguously that responsibility for regulatory compliance ultimately resides with the FSI, and the risk management guidance is designed to help FSIs assess the ability of a CSP to host the FSI's systems and support its compliance with all applicable regulatory requirements. The significant growth in the use of the public cloud by FSIs demonstrates that Google can successfully provide a secure cloud environment that supports compliance with FSIs' regulatory compliance obligations.

However, the regulators' guidance does not and cannot cover every conceivable situation where a potential regulatory issue is identified in a cloud migration effort or, alternatively in a post-migration situation, where a regulator raises an issue or question about either the cloud migration process, or a specific issue involving a system that moved from an on-premises' data center to a public cloud. As a general rule, the following considerations are useful in assessing the issues, identifying responsive materials, and responding to regulators' concerns in a timely way:

1. Has the FSI conducted a thorough risk assessment process that identified the key risks and corresponding mitigating controls, and are they fully documented?
2. During the cloud migration process, has the FSI's Legal / Compliance / Risk / Privacy / Information Security / Application Security staff been involved in reviewing the relevant documents to assure they align with regulatory and operating requirements?
3. Have the Board of Directors and key executives in the areas responsible for all aspects of the cloud migration been fully apprised of the progress and status of the migration pre-implementation, and have they been kept fully informed of all governance, supervision and control procedures and processes on an ongoing basis post-migration?
4. Is there a defined escalation path for raising system performance issues in cloud-based applications and assuring that appropriate personnel are timely and fully informed?

5. Has the FSI taken full advantage of available CSP native tools to enhance its own monitoring processes?
6. Does the FSI have protocols in place to interface with its CSP to identify potential issues? Are these protocols designed to assure an effective incident management response and documented in the contract with the CSP, as well as in the FSI's policies and procedures?
7. Have the FSI and the CSP continued to assess their respective controls around new system development projects to assure that there is the appropriate level of communication and coordination?
8. Consistent with an FSI's recordkeeping obligations under relevant laws, rules and regulations, are the FSI's records stored in an appropriate manner and readily available for production upon a regulator's request?
9. For questions involving a potential issue in the CSP's system, are there communication protocols in place that permit the FSI to obtain information about the issue and report it to its regulator within required timeframes?

Conclusion

Google's cloud offerings provide an FSI with benefits such as increased efficiency, enhanced products and services and reduced costs. FSIs also have the ability to enhance the in-house systems that they are required to maintain to monitor the performance of their cloud-based applications and processes through the use of monitoring tools provided by the CSP. Importantly, as in any outsourced arrangement, the FSI must perform a risk assessment involving all relevant stakeholders within the organization prior to moving to the cloud. Regulatory guidance thus focuses on the need for robust due diligence, both pre-and post-migration to the cloud, with a particular emphasis on certain core considerations and the parties' respective obligations, and an ongoing risk management and governance control process to monitor and supervise the performance of the outsourced activity. Google is committed to working with its FSI customers to develop strong governance controls and an effective system of collaboration and communication to assure that its FSI customers can migrate to Google Cloud with confidence in the integrity, reliability, and resiliency of its systems and data.

Appendix 1 Inventory of current regulations applicable to FSI migration to the cloud

Banking Regulators

Regulator	Current Regulations/Guidance
Federal Reserve	**Guidance on Managing Outsourcing Risk, December 2013** Supervisory Letter SR 13-19 / CA 13-21 on Guidance on Managing Outsourcing Risk -- December 5, 2013
	Bank Holding Company Supervision Manual, Section 2060.05.01, An Effective System of Internal Controls Bank Holding Company Supervision Manual
FDIC	**Regulatory Compliance and Risk Management Supervision – Financial Institution Letters** FIL-19-2019: Technology Service Provider Contracts FIL-13-2014 Technology Outsourcing Informational Tools for Community Bankers, FIL-44-2008 Guidance for Managing Third-Party Risk

Office of Comptroller of the Currency	Third-party Relationships: Risk Management Guidance Third-Party Relationships: Risk Management Guidance | OCC Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29
FFIEC	FFIEC Examination Handbook FFIEC IT Examination Handbook FFIEC Joint Statement on Risk Management for Cloud Computing Services FDIC | FIL-52-2020: FFIEC Joint Statement on Risk Management for Cloud Computing Services

Securities Regulators

Regulator	Current Regulations/Guidance
Securities and Exchange Commission	Regulation Systems Compliance and integrity, 17 CFR Parts 240, 242, and 249 [Release No. 34-73639; File No. S7-01-13]. *Note: this regulation is applicable to national securities exchanges and to certain alternative trading systems* Federal Register :: Regulation Systems Compliance and Integrity Securities Exchange Act Regulation 240.17a-1 – Recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies, and the Municipal Securities Rulemaking Board 17 CFR § 240.17a-1 - Recordkeeping rule for national securities exchanges, national securities associations, registered clearing

	agencies and the Municipal Securities Rulemaking Board. | CFR | US Law | LII / Legal Information Institute Securities Exchange Act Regulation 17a-4 - Records to be preserved by certain exchange members, brokers and dealers 17 CFR § 240.17a-4 - Records to be preserved by certain exchange members, brokers and dealers. SEC Regulation S-P – Requires broker dealers to safeguard customer records and information. Firms are required to have written policies and procedures addressing administrative, technical, and physical safeguards for the protection of customer records and information 17 CFR § 248.30 - Procedures to safeguard customer records and information; disposal of consumer report information. | CFR | US Law
FINRA	Regulatory Notices 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Providers Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers Regulatory Notice 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) Regulatory Notice 21-29
	Cloud Computing in the Securities Industry, August 2021 Cloud Computing in the Securities Industry | FINRA.org

Commodities Regulator

Regulator	Current Regulations/Guidance
CFTC	Rule 1.31 - Retention and Production of Regulatory Records. The rule governs the requirements for record retention, including retention periods, and requirement to produce records 17 CFR § 1.31 - Books and records; keeping and inspection. - Content Details - CFR-2017-title17-vol1-sec1-31 17 CFR 37, 17 CFR 38, 17 CFR 39. Rule governs cybersecurity testing requirements for all DCMs, SEFs, and SDRs, along with clarification of other system safeguards rule. Additional provisions for covered DCMs and SDRs, establishing minimum frequency requirements for conducting certain types of cybersecurity testing, and requiring performance of certain tests by independent contractors 17 CFR Part 37 - SWAP EXECUTION FACILITIES 17 CFR 38 - DESIGNATED CONTRACT MARKETS - Content Details - CFR-2017-title17-vol1-part38 17 CFR 39 - DERIVATIVES CLEARING ORGANIZATIONS - Content Details - CFR-2009-title17-vol1-part39

Derivatives Regulator

Regulator	Current Regulations/Guidance
National Futures Association	Compliance Rules 2-9 and 2-36 and Interpretive Notice 9079, Members' use of Third-Party Service Providers; Compliance Rules 2-9, 2-36 and 2-49 and Interpretive Notice 9070, Information Systems Security Programs

	NFA Compliance Rule 2-9 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs NFA Compliance Rule 2-49 9070 - NFA Compliance rules 2-9, 2-36 and 2-49: Information Systems Security Programs

Appendix 2: Components of an effective risk management program for third-party vendor relationships

Component	What it Requires
Planning	An evaluation of the types and nature of risks in the proposed relationship and a plan to manage the relationship and its related risks
Due Diligence and Third-Party Selection	A review of, among other items, the third-party's strategies and goals, legal and regulatory compliance capabilities, financial condition, business experience, fee structure and incentives, qualifications and background of the third-party vendor's principals, the effectiveness of the third-party's own risk management, including policies, procedures and internal controls, information security, management and information systems, operational resilience, incident reporting and management programs, and physical security and environmental controls.
Contractual Obligations	A contract that clearly delineates the terms of the outsourcing arrangement and does not contain terms that could result in an unacceptable level of risk to the FSI
Operational Resilience and Business Continuity	The contract must provide for a continuation of the business function in the event of a problem affecting the third-party's operations, including degradations or interruptions resulting from natural disasters, intentional attacks, or human error
Notification of Changes to Contracted Activity	The contract with the third-party must sufficiently address notification to the FSI entity before making changes to the contracted activities, including implementing new or revised policies, processes and information technology. Therefore, there should be in place a notification protocol whereby the CSP will provide timely notice to the FSI of any system or process change affecting its hosted systems and provide documentation to the FSI upon its request.
Notification of Incidents or CSP Operational Changes	The contract should also sufficiently address the expectations for the third party to notify the FSI of significant operational changes or when the CSP experiences significant incidents. Depending on the entity and the applicable requirements for regulatory notification in case of a system outage or intrusion, the timeframes for notification by the CSP to the FSI could be very short. This would require the CSP to have appropriate internal controls to provide such notification within required timeframes.

Appendix 3: Stakeholder areas of influence

Stakeholder	Risk Management Areas of Influence
CTO/CIO Technology Planning and Development/Program Management Office	□ Planning □ Due Diligence and Third-Party Selection □ Contractual Obligations □ Operational Resilience and Business Continuity □ Ongoing Monitoring □ Notification of Changes to Contracted Activity □ Notification of Incidents or CSP Operational Changes
CISO/Information Security	□ Planning □ Due Diligence and Third-Party Selection □ Contractual Obligations □ Operational Resilience and Business Continuity □ Ongoing Monitoring □ Notification of Changes to Contracted Activity □ Notification of Incidents or CSP Operational Changes
Finance	□ Planning □ Due Diligence and Third-Party Selection
Procurement	□ Planning □ Due Diligence and Third-Party Selection
CCO/Regulatory Compliance	□ Planning □ Operational Resilience and Business Continuity □ Ongoing Monitoring □ Notification of Changes to Contracted Activity □ Notification of Incidents or CSP Operational Changes
Audit	□ Due Diligence and Third-Party Selection □ Contractual Obligations □ Ongoing monitoring
Legal	□ Due Diligence and Third-Party Selection □ Contractual Obligations □ Notification of Changes to Contracted Activity
Operations	□ Planning □ Contractual Obligations □ Ongoing Monitoring □ Operational Resilience and Business Continuity □ Notification of Changes to Contracted Activity □ Notification of Incidents or CSP Operational Changes