Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

This document is designed to help firms supervised by the Financial Industry Regulatory Authority (“**regulated entity**”) to consider Regulatory Notice 21-29 Vendor Management and Outsourcing (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Due Diligence, Vendor Onboarding, Supervision. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**II. Due Diligence**		
2.	Once a member firm decides to outsource an activity or function, it may want to consider some or all of the following questions in evaluating and selecting potential Vendors:	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below.	N/A
3.	**Due Diligence Approach**		
4.	• Does your firm engage key internal stakeholders (e.g., Compliance, Legal, IT or Risk Management) relevant to, and with the requisite experience to assess, the outsourcing decision?	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
5.	• What factors does your firm consider when conducting due diligence on potential Vendors? These may include, but are not limited to: a Vendors' financial condition, experience and reputation; familiarity with regulatory requirements, fee structure and incentives; the background of Vendors' principals, risk management programs, information security controls, and resilience.	Financial status • You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. • You can review Google's audited financial statements on Alphabet's Investor Relations page. Experience and Reputation • Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. Regulatory requirements See our SEC Compliance page for information about how Google can help support you with your compliance efforts for SEC Rule 17a-4(f), CFTC Rule 1.31(c)-(d), and FINRA Rule 4511(c).	N/A

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Fees Refer to your Google Cloud Financial Services contract. Prices and fee information are also publicly available on our SKUs page. Refer to our Pricing page for more information. Leadership Information about Google Cloud's leadership team is available on our Media Resources page. Risk management Refer to Row 7. Information Security Controls Refer to Row 19. Resilience Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations.	Regulator Information, Audit and Access
6.	• If a potential Vendor will be performing a function that is subject to regulatory requirements, how does your firm evaluate whether the Vendor has the ability to comply with applicable regulatory requirements and undertakings (e.g., Book and Records rules, including ESM Notification Requirements)?	See our SEC Compliance page for information about how Google can help support you with your compliance efforts for SEC Rule 17a-4(f), CFTC Rule 1.31(c)-(d), and FINRA Rule 4511(c).	N/A
7.	• Does your firm consider obtaining evaluations of prospective Vendors' SSAE 18, Type II, SOC 2 (System and Organization Control) reports (if available)? If so,	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a	Certifications and Audit Reports

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	who reviews the evaluations and how does your firm follow up on any identified concerns, including, for example, those related to cybersecurity?	regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001:2013 (Information Security Management Systems) -ISO/IEC 27017:2015 (Cloud Security) -ISO/IEC 27018:2014 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
8.	• Does your firm take a risk-based approach to vendor due diligence? Does the scope and depth of your firm's due diligence reflect the degree of risk associated with the activities or functions that will be outsourced?	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A
9.	• Does your firm evaluate the impact to your customers or firm if a Vendor fails to perform, for example, by not fulfilling a regulatory obligation? What measures can your firm put in place to mitigate that risk?	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Significant Developments
10.	• Does your firm assess the BCPs of prospective Vendors that would perform critical business, operational, risk management or regulatory activities or functions?	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
11.	• If a Vendor will likely be conducting activities or functions that require registration under FINRA rules, does your firm have a process for determining whether the Vendor's personnel will be appropriately qualified and registered?	This is a customer consideration.	N/A
12.	• Does your firm evaluate Vendors' controls and due diligence of Vendors' sub-contractors, particularly if the sub-contractor may have access to sensitive firm or customer non-public information or critical firm systems?	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors
13.	• Does your firm include individuals with the requisite expertise and experience in the due diligence process—including with respect to cybersecurity, information technology, risk management, business functions and relevant regulatory obligations—to effectively evaluate potential Vendors? How does your firm handle instances where your firm does not have the expertise or experience in-house?	Refer to Rows 4 and 8.	N/A
14.	• Does your firm document its due diligence findings?	This is a customer consideration.	N/A
15.	• Conflicts of Interest – Does your firm put controls in place to mitigate potential conflicts of interest in the Vendor selection process? For example:		
16.	• Does your firm require staff involved in its Vendor selection processes to disclose any personal relationship with the Vendor? If so, what steps does your firm take to assess whether that relationship may influence the choice of Vendor?	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct.	N/A
17.	• Does your firm allow staff to receive compensation or gifts from potential or current Vendors, which could influence the decision to select, or maintain a relationship with, a particular Vendor?	See Row above.	N/A
18.	**Cybersecurity**		
19.	Does your firm assess the Vendors' ability to protect sensitive firm and customer non-public information and data? Does your firm have access to expertise to conduct that assessment? (See also question, above, regarding SSAE 18 Type II, SOC 2 reports.)	The security of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products	

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
20.	**III. Vendor Onboarding**		
21.	After completing due diligence and selecting a Vendor, firms may wish to consider putting in place a written contract with the Vendor that addresses, among other things, both the firm's and the Vendor's roles with respect to outsourced regulatory obligations.	The roles and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A
22.	**Vendor Contracts**		
23.	• Does your firm document relationships with Vendors in a written contract, and if not, under what circumstances?	The use of the Services is governed by the Google Cloud Financial Services Contract.	N/A
24.	• Do your firm's contracts address, when applicable, Vendors' obligations with respect to such issues as:		
25.	• documentation evidencing responsible parties' and Vendors' compliance with federal and state securities laws and regulations and FINRA rules (e.g., retention period required for preservation of firm records);	See our SEC Compliance page for information about how Google can help support you with your compliance efforts for SEC Rule 17a-4(f), CFTC Rule 1.31(c)-(d), and FINRA Rule 4511(c).	N/A
26.	• non-disclosure and confidentiality of information;	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Confidentiality
27.	• protection of non-public, confidential and sensitive firm and customer information;	Refer to Row 19.	N/A

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
28.	• ownership and disposition of firm and customer data at the end of the Vendor relationship;	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Intellectual Property Deletion on Termination (Cloud Data Processing Addendum)
29.	• notification to your firm of cybersecurity events and the Vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
30.	• Vendor BCP practices and participation in your firm's BCP testing, including frequency and availability of test results;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
31.	• disclosure of relevant pending or ongoing litigation;	Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
32.	• relationships between Vendors, sub-contractors and other third-parties;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
33.	• firm and regulator access to books and records; and	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access Customer Information, Audit and Access

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
34.	• timely notification to your firm of application or system changes that will materially affect your firm.	We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
35.	• Do your firm's contracts with Vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?	The obligations and duties of the parties are set out in the Google Cloud Financial Services Contract. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
36.	**Features and Default Settings of Vendor Tools**		
37.	• Does your firm review, and as appropriate adjust, Vendor tool default features and settings, such as to limit use of communication tools to specific firm-approved features (e.g., disabling a chat feature, or reviewing whether the communications are being captured for supervisory review), to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?	There are a number of ways to perform effective access / configuration management using the services: Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.	N/A
38.	**IV. Supervision**		
39.	Member firms have a continuing responsibility to oversee, supervise and monitor the Vendor's performance of the outsourced activity or function. Firms may wish to consider the following potential steps in determining how they fulfill this supervisory obligation:		

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
40.	• Obtaining representations from the Vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001:2013 (Information Security Management Systems) -ISO/IEC 27017:2015 (Cloud Security) -ISO/IEC 27018:2014 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
41.	• Requiring Vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;	You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
42.	• Going onsite to Vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Customer Information, Audit and Access
43.	• Monitoring and assessing the accuracy and quality of the Vendor's work product;	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected	Ongoing Performance Monitoring

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
44.	• Remaining aware of news of Vendor deficiencies and investigating whether they are indicative of a problem with an activity or function the Vendor is performing for your firm;	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
45.	• Investigating customer complaints that may be indicative of issues with a Vendor and exploring whether there are further-reaching impacts; and	Given the nature of the services, Google does not have direct interaction with the regulated entity's customers.	N/A
46.	• Training staff to address and escalate red flags at your firm that a Vendor may not be performing an activity or function adequately, such as not receiving confirmation that a Vendor task was completed.	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	N/A
47.	In addition to the above, firms may want to consider asking the following questions, where applicable, with respect to more specific aspects of their supervisory system.	This is a customer consideration.	N/A
48.	**Supervisory Control System**		
49.	• Does your firm monitor Vendors (for example, by reviewing SOC 2 reports) and document results of its ongoing supervision, especially for critical business or regulatory activities or functions?	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
50.	• Do your firm's WSPs address roles and responsibilities for firm staff who supervise Vendor activities?	This is a customer consideration.	
51.	• Does your firm periodically review and update its Vendor management-related WSPs to reflect material changes in the firm's business or business practices?	This is a customer consideration.	N/A
52.	**Business Continuity Planning**		
53.	• Does your firm's business continuity planning and testing include Vendors? If so, what are the testing requirements for Vendors and how often are such tests performed? How do these tests inform your firm's overall BCP?	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
54.	• Does your firm have contingency plans for interruptions or terminations of Vendor services?	Google recognizes that, whatever the level of technical resilience that can be achieved on GCP, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: -Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. -Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. -Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
55.	• If there is a disaster recovery event, has your firm assessed whether the Vendor will have sufficient staff dedicated to your firm?	Resilience Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications Staff Customers can operate the services independently without action by Google personnel. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there are no Google personnel dedicated to delivering the services to an individual customer. Google will ensure that Google personnel who are relevant to the maintenance and implementation of our business continuity plan are appropriately trained and aware of their roles and responsibilities. Additionally, Google will maintain procedures designed to ensure that all Google personnel can internally report and escalate such disasters and other events.	Business Continuity and Disaster Recovery
56.	**Cybersecurity and Technology Change Controls**		
57.	• **Access Controls**		
58.	• Does your firm know which Vendors have access to: (1) sensitive firm or customer non-public information and (2) critical firm systems?	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account.	Protection of Customer Data

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
59.	• Does your firm implement access controls through the lifecycle of its engagement with Vendors, including developing a "policy of least privilege" to grant Vendors system and data access only when required and revoke it when no longer needed and upon termination?	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data.	Data Security; Additional Security Controls (Cloud Data Processing Addendum) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum) Deletion by Customer (Cloud Data Processing Addendum)

Financial Industry Regulatory Authority - Regulatory Notice 21-29

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
60.	• Has your firm considered implementing multi-factor authentication for Vendors and, if warranted, their sub-contractors?	Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Refer to our Multi-Factor Authentication page for more information.	N/A
61.	• **Cybersecurity Events and Data Breaches**		
62.	• Does your firm conduct independent, risk-based reviews to determine if Vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the Vendors' response to such events?	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
63.	• If a cybersecurity breach occurred at your firm's Vendor, was your firm notified and, if so, how quickly? Did your firm follow its incident response plan for addressing such breaches?	Refer to Row 62.	N/A
64.	• **Technology Change Management**		
65.	• If applicable, how does your firm become aware of, evaluate and, as appropriate, test the impact of changes Vendors make to their applications and systems, especially for critical applications and systems?	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also control changes to your use of the services. Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services