Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

This document is designed to help banking organizations supervised by the Federal Banking Agencies ("**regulated entity**") to consider the Interagency Guidance on Third-Party Relationships: Risk Management ("**framework**") in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Chapter IV. Text of Final Interagency Guidance on Third-Party Relationships - Part C (Third-Party Relationship Life Cycle), Section 2 (Due Diligence and Third-Party Selection), Section 3 (Contract Negotiation), Section 4 (The Right to Audit and Require Remediation) and Section 5 (Termination). 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	**Part C, Section 2 (Due Diligence and Third-Party Selection)**		
2	**2. Due Diligence and Third-Party Selection:** Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management. It provides management with the information needed about potential third parties to determine if a relationship would help achieve a banking organization's strategic and financial goals. The due diligence process also provides the banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship. Due diligence includes assessing the third party's ability to: perform the activity as expected, adhere to a banking organization's policies related to the activity, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner. Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence, as due diligence should be tailored to the specific activity to be performed by the third party. The scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More comprehensive due diligence is particularly important when a third party supports higher-risk activities, including critical activities. If a banking organization uncovers information that warrants additional scrutiny, the banking organization should consider broadening the scope or assessment methods of the due diligence. In some instances, a banking organization may not be able to obtain the desired due diligence information from a third party. For example, the third party may not have a long operational history, may not allow on-site visits, or may not share (or be permitted to share) information that a banking organization requests. While the methods and scope of due diligence may differ, it is important for the banking organization to identify and document any limitations of its due diligence, understand the risks from such limitations, and consider alternatives as to how to mitigate the risks. In such situations, a banking organization may, for example, obtain alternative information to assess the third party, implement additional controls on or monitoring of the third party to address the information limitation, or consider using a different third party. A banking organization may use the services of industry utilities or consortiums, consult with other organizations, or engage in joint efforts to supplement its due diligence. As the activity to be performed by the third party may present a different level of risk to each banking organization, it is important to evaluate the conclusions from such supplemental efforts based on the banking organization's own specific circumstances and performance criteria for the activity. Effective risk management processes include evaluating the capabilities of any external party conducting the supplemental efforts, understanding	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. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page.	N/A

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	how such supplemental efforts relate to the banking organization's planned use of the third party, and assessing the risks of relying on the supplemental efforts. Use of such external parties to conduct supplemental due diligence does not abrogate the responsibility of the banking organization to manage third-party relationships in a safe and sound manner and consistent with applicable laws and regulations. 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 due diligence:		
3	**a. Strategies and Goals:** A review of the third party's overall business strategy and goals helps the banking organization to understand: (1) how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, and partnerships) may affect the activity; and (2) the third party's service philosophies, quality initiatives, and employment policies and practices (including its diversity policies and practices). Such information may assist a banking organization to determine whether the third party can perform the activity in a manner that is consistent with the banking organization's broader corporate policies and practices.	Strategy Information about Google's strategy is available on Alphabet's Investor Relations page. Philosophies 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
4	**b. Legal and Regulatory Compliance:** A review of any legal and regulatory compliance considerations associated with engaging a third party allows a banking organization to evaluate whether it can appropriately mitigate risks associated with the third-party relationship. This may include (1) evaluating the third party's ownership structure (including identifying any beneficial ownership, whether public or private, foreign, or domestic ownership) and whether the third party has the necessary legal authority to perform the activity, such as any necessary licenses or corporate powers; (2) determining whether the third party itself or any owners are subject to sanctions by the Office of Foreign Assets Control; (3) determining whether the third party has the expertise, processes, and controls to enable the banking organization to remain in compliance with applicable domestic and international laws and regulations; (4) considering the third party's responsiveness to any compliance issues (including violations of law or regulatory actions) with applicable supervisory agencies and self-regulatory organizations, as appropriate; and (5) considering whether the third party has identified, and articulated a process to mitigate, areas of potential consumer harm.	Corporate information You can review Google's corporate and financial information on Alphabet's Investor Relations page. Compliance As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information.	
5	**c. Financial Condition:** An assessment of a third party's financial condition through review of available financial information, including audited financial statements, annual	You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	reports, and filings with the U.S. Securities and Exchange Commission (SEC), among others, helps a banking organization evaluate whether the third party has the financial capability and stability to perform the activity.		
6	Where relevant and available, a banking organization may consider other types of information such as access to funds, expected growth, earnings, pending litigation, unfunded liabilities, reports from debt rating agencies, and other factors that may affect the third party's overall financial condition.	Expected growth Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page. Pending litigation Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
7	**d. Business Experience:** An evaluation of a third party's: (1) depth of resources (including staffing); (2) previous experience in performing the activity; and (3) history of addressing customer complaints or litigation and subsequent outcomes, helps to inform a banking organization's assessment of the third party's ability to perform the activity effectively. Another consideration may include whether there have been significant changes in the activities offered or in its business model. Likewise, a review of the third party's websites, marketing materials, and other information related to banking products or services may help determine if statements and assertions accurately represent the activities and capabilities of the third party.	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.	N/A
8	**e. Qualifications and Backgrounds of Key Personnel and Other Human Resources Considerations:** An evaluation of the qualifications and experience of a third party's principals and other key personnel related to the activity to be performed provides insight into the capabilities of the third party to successfully perform the activities. An important consideration is whether the third party and the banking organization, as appropriate,	Principals Information about Google Cloud's leadership team is available on our Media Resources page.	

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	periodically conduct background checks on the third party's key personnel and contractors who may have access to information technology systems or confidential information. Another important consideration is whether there are procedures in place for identifying and removing the third party's employees who do not meet minimum suitability requirements or are otherwise barred from working in the financial services sector. Another consideration is whether the third party has training to ensure that its employees understand their duties and responsibilities and are knowledgeable about applicable laws and regulations as well as other factors that could affect performance or pose risk to the banking organization. Finally, an evaluation of the third party's succession and redundancy planning for key personnel, and of the third party's processes for holding employees accountable for compliance with policies and procedures, provides valuable information to the banking organization.	Background checks Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. Training All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Refer to our security whitepaper for more information. 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. Business continuity Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware. Employee policies 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, which addresses conflicts of interest.	Personnel Security, Appendix 2: Security Measures (Cloud Data Processing Addendum)
9	**f. Risk Management:** Appropriate due diligence includes an evaluation of the effectiveness of a third party's overall risk management, including policies, processes, and internal controls, and alignment with applicable policies and expectations of the banking organization surrounding the activity. This would include an assessment of the third party's governance processes, such as the establishment of clear roles, responsibilities, and segregation of duties pertaining to the activity. It is also important to consider whether the third party's controls and operations are subject to effective audit assessments, including independent testing and objective reporting of results and findings. Banking organizations also gain important insight by evaluating processes for	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	Certifications and Audit Reports

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	escalating, remediating, and holding management accountable for concerns identified during audits, internal compliance reviews, or other independent tests, if available. When relevant and available, a banking organization may consider reviewing System and Organization Control (SOC) reports and any conformity assessment or certification by independent third parties related to relevant domestic or international standards. In such cases, the banking organization may also consider whether the scope and the results of the SOC reports, certifications, or assessments are relevant to the activity to be performed or suggest that additional scrutiny of the third party or any of its contractors may be appropriate.	• 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.	
10	**g. Information Security:** Understanding potential information security implications, including access to a banking organization's systems and information, can help a banking organization decide whether or not to engage with a third party. Due diligence in this area typically involves assessing the third party's information security program, including its consistency with the banking organization's information security program, such as its approach to protecting the confidentiality, integrity, and availability of the banking organization's data. It may also involve determining whether there are any gaps that present risk to the banking organization or its customers and considering the extent to which the third party applies controls to limit access to the banking organization's data and transactions, such as multifactor authentication, end-to-end encryption, and secure source code management.	Information security The security / confidentiality 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. 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.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(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 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	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Access controls 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.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
11	It also aids a banking organization when determining whether the third party keeps informed of, and has sufficient experience in identifying, assessing, and mitigating, known and emerging threats and vulnerabilities. As applicable, assessing the third party's data, infrastructure, and application security programs, including the software development life cycle and results of vulnerability and penetration tests, can provide	Vulnerability tests Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	valuable information regarding information technology system vulnerabilities. Finally, due diligence can help a banking organization evaluate the third party's implementation of effective and sustainable corrective actions to address any deficiencies discovered during testing.	processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our security whitepaper for more information. Penetration testing You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Customer Penetration Testing
12	**h. Management of Information Systems:** It is important to review and understand the third party's business processes and information systems that will be used to support the activity. When technology is a major component of the third-party relationship, an effective practice is to review both the banking organization's and the third party's information systems to identify gaps in service-level expectations, business process and management, and interoperability issues. It is also important to review the third party's processes for maintaining timely and accurate inventories of its technology and its contractor(s). A banking organization also benefits from understanding the third party's measures for assessing the performance of its information systems.	Documentation Refer to our Documentation page for technical documentation, including information on service configuration. Service Levels The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Interoperability There are a number of ways to integrate our services with your systems: • Cloud Console allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage. • Cloud APIs allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language.	Services

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Technology inventory Google centralizes control of our software supply chain and actively secures each step of the end-to-end process. We start by maintaining separate secured copies of the source code for our dependencies and perform our own vulnerability scanning. Most of our source code is stored in a central monolithic repository, which enables employees to check code into a single location. The Google codebase simplifies source code management, in particular management of our dependencies on third-party code. A monolithic codebase also allows for the enforcement of a single choke point for code reviews. We continuously fuzz 550 of the most commonly-used open source projects. We then manage an end-to-end build, deploy, and distribution process that includes integrated integrity, provenance, and security checks. In addition: ● Based on our internal security practices, Binary Authorization for Borg, we have created the SLSA framework to enable organizations to assess the maturity of their software supply chain security and understand key steps to progress to the next level. SLSA lays out an actionable path for organizations to increase their overall software supply-chain security by providing step-by-step guidelines and practical goals for protecting source and build system integrity. The SLSA framework addresses a limitation of Software Bills of Materials (SBOMs), which on their own do not provide sufficient information about integrity and provenance. ● Assured OSS allows enterprise customers to directly benefit from the in-depth, end-to-end security capabilities and practices we apply to our own OSS portfolio by providing access to the same OSS packages that Google depends on.	
13	**i. Operational Resilience:** An assessment of a third party's operational resilience practices supports a banking organization's evaluation of a third party's ability to effectively operate through and recover from any disruption or incidents, both internal and external. Such an assessment is particularly important where the impact of such disruption could have an adverse effect on the banking organization or its customers,	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	

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	including when the third party interacts with customers. It is important to assess options to employ if the third party's ability to perform the activity is impaired and to determine whether the third party maintains appropriate operational resilience and cybersecurity practices, including disaster recovery and business continuity plans that specify the time frame to resume activities and recover data.	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. Business Continuity Plan 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
14	To gain additional insight into a third party's resilience capabilities, a banking organization may review (1) the results of operational resilience and business continuity testing and performance during actual disruptions; (2) the third party's telecommunications redundancy and resilience plans; and (3) preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, pandemics, distributed denial of service attacks, or other intentional or unintentional events. Other considerations related to operational resilience include (1) dependency on a single provider for multiple activities; and (2) interoperability or potential end of life issues with the software programming language, computer platform, or data storage technologies used by the third party.	Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including: • destruction of infrastructure required to provide the Services • interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures) • unavailability of key personnel • emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) pandemicsYou can review information about Google's historic performance of the services on our Google Cloud Service Health Dashboard.	Business Continuity and Disaster Recovery

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	Data Export (Cloud Data Processing Addendum)
15	**j. Incident Reporting and Management Processes:** Review and consideration of a third party's incident reporting and management processes is helpful to determine whether there are clearly documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents. Such review assists in confirming that the third party's escalation and notification processes meet the banking organization's expectations and regulatory requirements.	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)
16	**k. Physical Security:** It is important to evaluate whether the third party has sufficient physical and environmental controls to protect the safety and security of people (such as employees and customers), its facilities, technology systems, and data, as applicable. This would typically include a review of the third party's employee on- and off-boarding procedures to ensure that physical access rights are managed appropriately.	Refer to Row 10 for more information on Google's security measures regarding your data.	N/A
17	**l. Reliance on Subcontractors:** An evaluation of the volume and types of subcontracted activities and the degree to which the third party relies on subcontractors helps inform whether such subcontracting arrangements pose additional or heightened risk to a banking organization. This typically includes an assessment of the third party's ability to identify, manage, and mitigate risks associated with subcontracting, including how the	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;	Google Subcontractors

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	third party selects and oversees its subcontractors and ensures that its subcontractors implement effective controls. Other important considerations include whether additional risk is presented by the geographic location of a subcontractor or dependency on a single provider for multiple activities.	• 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 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.	
18	**m. Insurance Coverage:** An evaluation of whether the third party has existing insurance coverage helps a banking organization determine the extent to which potential losses are mitigated, including losses posed by the third party to the banking organization or that might prevent the third party from fulfilling its obligations to the banking organization. Such losses may be attributable to dishonest or negligent acts; fire, floods, or other natural disasters; loss of data; and other matters. Examples of insurance coverage may include fidelity bond; liability; property hazard and casualty; and areas that may not be covered under a general commercial policy, such as cybersecurity or intellectual property.	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
19	**n. Contractual Arrangements with Other Parties:** A third party's commitments to other parties may introduce potential legal, financial, or operational implications to the banking organization. Therefore, it is important to obtain and evaluate information regarding the third party's legally binding arrangements with subcontractors or other parties to determine whether such arrangements may create or transfer risks to the banking organization or its customers.	Refer to Row 17 on subcontractors.	N/A
20	**Part C: Section 3 (Contract Negotiation)**		
21	**3. Contract Negotiation:** When evaluating whether to enter into a relationship with a third party, a banking organization typically determines whether a written contract is needed, and if the proposed contract can meet the banking organization's business goals and risk management needs. After such determination, a banking organization typically negotiates contract provisions that will facilitate effective risk management and oversight and that specify the expectations and obligations of both the banking organization and the third party. A banking organization may tailor the level of detail and	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate	Enabling Customer Compliance

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	comprehensiveness of such contract provisions based on the risk and complexity posed by the particular third-party relationship. While third parties may initially offer a standard contract, a banking organization may seek to request modifications, additional contract provisions, or addendums to satisfy its needs. In difficult contract negotiations, including when a banking organization has limited negotiating power, it is important for the banking organization to understand any resulting limitations and consequent risks. Possible actions that a banking organization might take in such circumstances include determining whether the contract can still meet the banking organization's needs, whether the contract would result in increased risk to the banking organization, and whether residual risks are acceptable. If the contract is unacceptable for the banking organization, it may consider other approaches, such as employing other third parties or conducting the activity in-house. In certain circumstances, banking organizations may gain an advantage by negotiating contracts as a group with other organizations. It is important that a banking organization understand the benefits and risks associated with engaging third parties and particularly before executing contracts involving higher-risk activities, including critical activities. As part of its oversight responsibilities, the board of directors should be aware of and, as appropriate, may approve or delegate approval of contracts involving higher-risk activities. Legal counsel review may also be warranted prior to finalization. Periodic reviews of executed contracts allow a banking organization to confirm that existing provisions continue to address pertinent risk controls and legal protections. If new risks are identified, a banking organization may consider renegotiating a contract. Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, during contract negotiations:	that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	
22	**a. Nature and Scope of Arrangement:** In negotiating a contract, it is helpful for a banking organization to clearly identify the rights and responsibilities of each party. This typically includes specifying the nature and scope of the business arrangement. Additional considerations may also include, as applicable, a description of (1) ancillary services such as software or other technology support, maintenance, and customer service; (2) the activities the third party will perform; and (3) the terms governing the use of the banking organization's information, facilities, personnel, systems, intellectual property, and equipment, as well as access to and use of the banking organization's or customers'	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract. Scope The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	N/A Services

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	information. If dual employees will be used, it may also be helpful to specify their responsibilities and reporting lines. It is also important for a banking organization to understand how changes in business and other circumstances may give rise to the third party's rights to terminate or renegotiate the contract.	Support The support services are described on our Technical Support Services Guidelines page. Information Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising	Technical Support Protection of Customer Data
23	**b. Performance Measures or Benchmarks:** For certain relationships, clearly defined performance measures can assist a banking organization in evaluating the performance of a third party. In particular, a service-level agreement between the banking organization and the third party can help specify the measures surrounding the expectations and responsibilities for both parties, including conformance with policies and procedures and compliance with applicable laws and regulations. Such measures can be used to monitor performance, penalize poor performance, or reward outstanding performance. It is important to negotiate performance measures that do not incentivize imprudent performance or behaviour, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on the banking organization or customers.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Services
24	**c. Responsibilities for Providing, Receiving, and Retaining Information:** 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:		
25	• The banking organization's ability to access its data in an appropriate and timely manner;	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 and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Regulator Information, Audit and Access
26	• The banking organization's access to, or use of, the third-party's data and any supporting documentation, in connection with the business arrangement;	Google provides documentation to explain how institutions and their employees can use our services. If an institution would like more guided training, Google also provides a variety of courses and certifications.	

Interagency Guidance on Third-Party Relationships: Risk Management

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.	Certifications and Audit Reports
27	• The banking organization's access to, or use of, its own or the third-party's data and how such data and supporting documentation may be shared with regulators in a timely manner as part of the supervisory process;	Refer to Rows 25 and 26.	N/A
28	• 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;	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Intellectual Property Protection of Customer Data
29	• Notification to the banking organization whenever compliance lapses, enforcement actions, regulatory proceedings, or other events pose a significant risk to the banking organization or customers;	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	• 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; and	Refer to Row 29 on significant developments. Mergers, acquisition, divestitures Google will provide advance notice to you if it experiences a relevant change in control. Subcontractors 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;	Change of Control Google Subcontractors

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor. Key personnel 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.	
31	• 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.	Performance reports 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 Service Health 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. Financial reports You can review Google's audited financial statements on Alphabet's Investor Relations page. Google provides billing tools that customers can use to obtain reports on their usage of the Services and associated costs. More information is available on our Cloud Billing documentation page and the Export Cloud Billing data to BigQuery page. Security reports Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. Google publishes Threat Horizons intelligence reports to help keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat	Ongoing Performance Monitoring Customer Penetration Testing

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud Platform Services, via https://cloud.google.com/support/bulletins Control assessments 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
32	**d. The Right to Audit and Require Remediation:** To help ensure that a banking organization has the ability to monitor the performance of a third party, a contract often establishes the banking organization's right to audit and provides for remediation when issues are identified. Generally, a contract includes provisions for periodic, independent audits of the third party and its relevant subcontractors, consistent with the risk and complexity of the third-party relationship. Therefore, it would be appropriate to consider whether contract provisions describe the types and frequency of audit reports the banking organization is entitled to receive from the third party (for example, SOC reports, Payment Card Industry (PCI) compliance reports, or other financial and operational reviews). 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.	Independent third party audits 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. Google is audited at least once a year for each audited framework. Google performs planning, scoping and readiness activities prior to each audit. Audit by the banking organization 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.	Certifications and Audit Reports Enabling Customer Compliance

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls. Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
33	**e. Responsibility for Compliance with Applicable Laws and Regulations:** A banking organization is responsible for conducting its activities in compliance with applicable laws and regulations, including those activities involving third parties. The use of third parties does not abrogate these responsibilities. Therefore, it is important for a contract to specify the obligations of the third party and the banking organization to comply with applicable laws and regulations.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
34	It is also important for the contract to provide the banking organization with the right to monitor and be informed about the third party's compliance with applicable laws and regulations, and to require timely remediation if issues arise. Contracts may also reflect considerations of relevant guidance and self-regulatory standards, where applicable.	Ongoing monitoring 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 Service Health 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. Significant developments 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.	Ongoing Performance Monitoring Significant Developments

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
35	**f. Costs and Compensation:** Contracts that clearly describe all costs and compensation arrangements help reduce misunderstandings and disputes over billing and help ensure that all compensation arrangements are consistent with sound banking practices and applicable laws and regulations. Contracts commonly describe compensation and fees, including cost schedules, calculations for base services, and any fees based on volume of activity and for special requests. Contracts also may specify the conditions under which the cost structure may be changed, including limits on any cost increases. During negotiations, a banking organization should confirm that a contract does not include incentives that promote inappropriate risk taking by the banking organization or the third party.	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.	Payment Terms
36	A banking organization should also consider whether the contract includes burdensome upfront or termination fees, or provisions that may require the banking organization to reimburse the third party. Appropriate provisions indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Another consideration is outlining cost and responsibility for purchasing and maintaining hardware and software, where applicable.	Google is committed to supporting regulated entities with audits of our services. As this support is not included in our usual publicly listed service fees, Google may charge an additional fee in connection with an audit. Google will provide further details of any fee in advance of the activity when the scope of the activity is known.	Enabling Customer Compliance; Fee
37	**g. Ownership and License:** In order to prevent disputes between the parties regarding the ownership and licensing of a banking organization's property, it is common for a contract to state the extent to which the third party has the right to use the banking organization's information, technology, and intellectual property, such as the banking organization's name, logo, trademark, and copyrighted material. Provisions that indicate whether any data generated by the third party become the banking organization's property help avert misunderstandings. It is also important to include appropriate warranties on the part of the third party related to its acquisition of licenses or subscriptions for use of any intellectual property developed by other third parties. When the banking organization purchases software, it is important to consider a provision to establish escrow agreements to provide for the banking organization's access to source code and programs under certain conditions (for example, insolvency of the third party).	Intellectual property 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. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Google will not use your copyright, patent, trademark or logo without your prior approval. Third party software Refer to the Google Cloud Service Specific Terms. Escrow Our services are one-to-many. This means that Google uses the same underlying technology to provide the services to all our Google Cloud customers. To ensure service continuity for all of our customers (including other regulated entities), we cannot enter into source code escrow agreements with any individual customer. However, we recognize the importance of continuity for regulated entities and for this reason we are	Intellectual Property Protection of Customer Data Marketing and Publicity

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		committed to data portability and open-source. Refer to our Open Cloud page for more information on Google's approach to open source.	
38	**h. Confidentiality and Integrity:** With respect to contracts with third parties, there may be increased risks related to the sensitivity of non-public information or access to infrastructure. Effective contracts typically prohibit the use and disclosure of banking organization and customer information by a third party and its subcontractors, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives personally identifiable information, contract provisions are important to ensure that the third party implements and maintains appropriate security measures to comply with applicable laws and regulations. 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. Considerations may include the types of data stored by the third party, legal obligations for the banking organization to disclose the breach to its regulators or customers, the potential for consumer harm, or other factors. 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. They also address the powers of each party to change security and risk management procedures and requirements and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Typically, such provisions stipulate whether and how often the banking organization and the third party will jointly practice incident management exercises involving unauthorized intrusions or other breaches of confidentiality and integrity.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. In particular, Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Google continues to improve the security of 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, these updates apply to all customers at the same time. Google will not update our security measures in a way that results in a material reduction of the security of the services. Refer to Row 10 on how you can configure the services to address your security and risk management requirements. 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. To assist customers with their own incident response, Google's notification will describe: ● the nature of the Data Incident including the Customer resources impacted; ● the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; ● the measures, if any, Google recommends that Customer take to address the Data Incident; and ● details of a contact point where more information can be obtained.	Protection of Customer Data, Data Security; Google's Security Measures (Cloud Data Processing Addendum) Data Incidents (Cloud Data Processing Addendum)
39	**i. Operational Resilience and Business Continuity:** Both internal and external factors or incidents (for example, natural disasters or cyber incidents) may affect a banking organization or a third party and thereby disrupt the third party's performance of the activity. Consequently, an effective contract provides for continuation of the activity in the event of problems affecting the third party's operations, including degradations or interruptions in delivery. As such, it is important for the contract to address the third	Service continuity Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper.	Business Continuity and Disaster Recovery

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	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. To help ensure maintenance of operations, contracts often require the third party to provide the banking organization with operating procedures to be carried out in the event business continuity plans are implemented, including specific recovery time and recovery point objectives. Contracts may also stipulate whether and how often the banking organization and the third party will jointly test business continuity plans. Another consideration is whether the contract provides for the transfer of the banking organization's accounts, data, or activities to another third party without penalty in the event of the third party's bankruptcy, business failure, or business interruption.	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. In particular, refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. 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. Exit Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. 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.	Transition Term Data Export (Cloud Data Processing Addendum)

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a 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.	
40	**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.	Indemnification Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract. Liability Refer to your Google Cloud Financial Services Contract.	Indemnification Liability
41	**k. Insurance:** One way in which a banking organization can protect itself against losses caused by or related to a third party and the products and services provided through third-party relationships is by including insurance requirements in a contract. These provisions typically require the third party to (1) maintain specified types and amounts of insurance (including, if appropriate, naming the banking organization as insured or additional insured); (2) notify the banking organization of material changes to coverage; and (3) provide evidence of coverage, as appropriate. The type and amount of insurance coverage should be commensurate with the risk of possible losses, including those caused by the third party to the banking organization or that might prevent the third party from fulfilling its obligations to the banking organization, and the activities performed.	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
42	**l. Dispute Resolution:** Disputes regarding a contract can delay or otherwise have an adverse impact upon the activities performed by a third party, which may negatively affect the banking organization. Therefore, a banking organization may want to consider whether the contract should establish a dispute resolution process to resolve problems between the banking organization and the third party in an expeditious manner, and	Refer to your Google Cloud Financial Services Contract.	Governing Law

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	whether the third party should continue to provide activities to the banking organization during the dispute resolution period. It is important to also understand whether the contract contains provisions that may impact the banking organization's ability to resolve disputes in a satisfactory manner, such as provisions addressing arbitration or forum selection.		
43	**m. Customer Complaints:** Where customer interaction is an important aspect of the third-party relationship, a banking organization may find it useful to include a contract provision to ensure that customer complaints and inquiries are handled properly. Effective contracts typically specify whether the banking organization or the third party is responsible for responding to customer complaints or inquiries. If it is the third party's responsibility, it is important to include provisions for the third party to receive and respond to customer complaints and inquiries in a timely manner and to provide the banking organization with sufficient, timely, and usable information to analyse customer complaint and inquiry activity and associated trends. If it is the banking organization's responsibility, it is important to include provisions for the banking organization to receive prompt notification from the third party of any complaints or inquiries received by the third party.	Given the nature of the services, Google does not have direct interaction with the regulated entity's customers.	N/A
44	**n. Subcontracting:** Third-party relationships may involve subcontracting arrangements, which can result in risk due to the absence of a direct relationship between the banking organization and the subcontractor, further lessening the banking organization's direct control of activities. The impact on a banking organization's ability to assess and control risks may be especially important if the banking organization uses third parties for higher-risk activities, including critical activities. For this reason, a 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. Another important consideration is whether the contract should prohibit assignment, transfer, or subcontracting of the third party's obligations to another entity without the banking organization's consent. 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. Where appropriate, a banking organization may consider including a provision that states the third party's liability for activities or actions by its subcontractors and which party is	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting arrangement. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice. 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

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	responsible for the costs and resources required for any additional monitoring and management of the subcontractors. It may also be appropriate to reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with contractual obligations.	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights) and applicable law and regulation. Google will remain liable to you for any subcontracted obligations.	
45	**o. Foreign-Based Third Parties:** In contracts with foreign-based third parties, it is important to consider choice-of-law and jurisdictional provisions that provide dispute adjudication under the laws of a single jurisdiction, whether in the United States or elsewhere. When engaging with foreign-based third parties, or where contracts include a choice-of-law provision that includes a jurisdiction other than the United States, it is important to understand that such contracts and covenants may be subject to the interpretation of foreign courts relying on laws in those jurisdictions. It may be warranted to seek legal advice on the enforceability of the proposed contract with a foreign-based third party and other legal ramifications, including privacy laws and cross-border flow of information.	Google LLC is the provider of the services for US-based regulated entities. Google LLC is organized under the laws of the State of Delaware, USA. Refer to your Google Cloud Financial Services Contract for more information about the governing law and jurisdiction that applies to our contract.	Governing Law
46	**p. Default and Termination:** Contracts can protect the ability of the banking organization to change third parties when appropriate without undue restrictions, limitations, or cost. 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:		
47	• 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;	Termination Regulated entities can elect to terminate our contract for convenience with advance notice, including: • if necessary to comply with law; • if directed by a supervisory authority; and • if Google increases the fees. Regulated entities can terminate our contract with advance notice: • for Google's material breach after a cure period • for change of control	Term and Termination

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• for Google's insolvency <u>Transition</u> Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.	Transition Term
48	• Provide for the timely return or destruction of the banking organization's data, information, and other resources;	Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. 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.	Data Export (Cloud Data Processing Addendum) Deletion on Termination (Cloud Data Processing Addendum)
49	• Assign all costs and obligations associated with transition and termination; and	The cost of migration is transparent and based on our publicly listed service fees. Our services enable you to transfer your data independently. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services subject to agreeing additional fees.	Transition Assistance
50	• 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.	Regulated entities can elect to terminate our contract for convenience with advance notice, including if directed by a supervisory authority.	Term and Termination

Interagency Guidance on Third-Party Relationships: Risk Management

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
51	**q. Regulatory Supervision:** 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.	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