OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

This document is designed to help national banks and federal savings associations supervised by the Office of the Comptroller of the Currency ("**banks**") to consider OCC Bulletin 2013-29 Third Party Relationship: Risk Management Guidance (the "**OCC Bulletin**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the OCC Bulletin: Due Diligence and Third Party Selection and Contract Negotiation. For each paragraph of these Sections, we provide commentary to help you understand how you can address the OCC Bulletin using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
1	**Due Diligence And Selection Of Service Providers**		
2	A bank should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner. The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is necessary when a third-party relationship involves critical activities. On-site visits may be useful to understand fully the third party's operations and capacity. If the bank uncovers information that warrants additional scrutiny, it should broaden the scope or assessment methods of the due diligence as needed. The bank should consider the following during due diligence:	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 information for each of the areas you need to consider in the rows that follow.	N/A
3	**Strategies and Goals**		
4	Review the third party's overall business strategy and goals to ensure they do not conflict with those of the bank. Consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, joint ventures, or joint marketing initiatives) may affect the activity. Also consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices.	Information about Google Cloud's strategies and goals is available on Alphabet's Investor Relations page. It also provides information about our organizational policies e.g. our Code of Conduct.	N/A
5	**Legal and Regulatory Compliance**		
6	Evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations as appropriate.	Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
7	**Financial Condition**		
8	Assess the third party's financial condition, including reviews of the third party's audited financial statements. Evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability. Depending	You can review our audited financial statements and information about Google's financial condition on Alphabet's Investor Relations page. This provides information	N/A

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	on the significance of the third-party relationship, the bank's analysis may be as comprehensive as if extending credit to the third party.	about our financial strength and sustainability, our areas of investment and growth as well as risk factors and details of material pending legal proceedings.	
9	**Business Condition and Reputation**		
10	Evaluate the third party's depth of resources and previous experience providing the specific activity. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model. Conduct reference checks with external organizations and agencies such as the industry associations, Better Business Bureau, Federal Trade Commission, state attorneys general offices, state consumer affairs offices, and similar foreign authorities. Check U.S. Securities and Exchange Commission or other regulatory filings. Review the third party's Websites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities. Determine whether and how the third party plans to use the bank's name and reputation in marketing efforts.	Business condition You can review information about our business condition on Alphabet's Investor Relations page. Reputation • Technology: Information about Google Cloud's technology and systems architecture is available on our Choosing Google Cloud page. • Qualifications and competencies: 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. • Reference customers: Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. • Performance record: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard.	N/A
11	**Fee Structure and Incentives**		
12	Evaluate the third party's normal fee structure and incentives for similar business arrangements to determine if the fee structure and incentives would create burdensome upfront fees or result in inappropriate risk taking by the third party or the bank.	Information about Google Cloud's pricing is available on our Pricing page.	N/A
13	**Qualifications, Backgrounds, and Reputations of Company Principals**		
14	Ensure the third party periodically conducts thorough background checks on its senior management and employees as well as on subcontractors who may have access to critical systems or confidential information. Ensure that third parties have policies and procedures in place for removing employees who do not meet minimum background check requirements.	Company principals Information about Google Cloud's leadership team is available on our Media Resources page. Background checks Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees.	N/A
15	**Risk Management**		
16	Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls. Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls. Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests. If available, review Service Organization Control (SOC) reports, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Consider whether these reports contain sufficient information to assess the third party's risk or whether	Google recognizes that banks need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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)	N/A

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	additional scrutiny is required through an audit by the bank or other third party at the bank's request. Consider any certification by independent third parties for compliance with domestic or international internal control standards (e.g., the National Institute of Standards and Technology and the International Standards Organization).	• 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.	
17	**Information Security**		
18	Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.	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 particular, refer to our security whitepaper on security monitoring and vulnerability management. In addition, refer to Row 16 for more information on the certifications and audit reports that Google maintains.	N/A
19	**Management of Information Systems**		
20	Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining accurate inventories of its technology and its subcontractors. Assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place. Understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations.	Refer to Row 16 for more information on the certifications and audit reports that Google maintains for its information systems.	N/A
21	**Resilience**		
22	Assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. Review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters,	Google recognizes the importance of business continuity and contingency planning. We do our own planning for our services. You can also use our services in your own business continuity and contingency planning. Google will implement a disaster recovery and business contingency plan for our services, review and test it at least annually and ensure it remains current with industry standards. Banks can review our plan and testing results.	N/A

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	distributed denial of service attacks, or other intentional or unintentional events. Review the results of business continuity testing and performance during actual disruptions.	In addition, information about how customers can use our Services in their own disaster recovery and business contingency planning is available in our Disaster Recovery Planning Guide.	
23	**Incident-Reporting and Management Programs**		
24	Review the third party's incident reporting and management programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents. Ensure that the third party's escalation and notification processes meet the bank's expectations and regulatory requirements.	Information on Google's data incident response process is available in our Data incident response whitepaper.	N/A
25	**Physical Security**		
26	Evaluate whether the third party has sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees.	Refer to Row 18 for information on Google's security practices.	N/A
27	**Human Resource Management**		
28	Review the third party's program to train and hold employees accountable for compliance with policies and procedures. Review the third party's succession and redundancy planning for key management and support personnel. Review training programs to ensure that the third party's staff is knowledgeable about changes in laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided.	Refer to Row 18 for information on Google's security practices. In particular, refer to our security whitepaper on Google's security culture.	N/A
29	**Reliance on Subcontractors**		
30	Evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third party's critical subcontractors.	Google recognizes that banks 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. To ensure banks retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice and Google will remain accountable to you for any subcontracted obligations. Refer to row 70.	N/A
31	**Insurance Coverage**		
32	Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents. Determine whether the third party has insurance coverage for its intellectual property rights, as such coverage may not be available under a general commercial policy. The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.	Google will maintain insurance cover against a number of identified risks.	Insurance
33	**Conflicting Contractual Arrangements With Other Parties**		

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

34	Obtain information regarding legally binding arrangements with subcontractors or other parties in cases where the third party has indemnified itself, as such arrangements may transfer risks to the bank. Evaluate the potential legal and financial implications to the bank of these contracts between the third party and its subcontractors or other parties.	Refer to Row 8 on Google's financial condition and row 70 on subcontractors.	N/A
35	Senior management should review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third-party relationship. If the results do not meet expectations, management should recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity. As part of any recommended changes, the bank may need to supplement the third party's resources or increase or implement new controls to manage the risks. Management should present results of due diligence to the board when making recommendations for third-party relationships that involve critical activities.	This is a customer consideration.	N/A
36	**Contract Negotiation**		
37	Once the bank selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. Additionally, senior management should obtain board approval of the contract before its execution when a third-party relationship will involve critical activities. A bank should review existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the bank should seek to renegotiate at the earliest opportunity. Contracts should generally address the following:	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A
38	**Nature and Scope of Arrangement**		
39	Ensure that the contract specifies the nature and scope of the arrangement. For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided. Include in the contract, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service. Specify which activities the third party is to conduct, whether on or off the bank's premises, and describe the terms governing the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information. When dual employees will be used, clearly articulate their responsibilities and reporting lines.	The GCP services are described on our services summary page. The support services are described on our technical support services guidelines page.	Definitions Technical Support
40	**Performance Measures or Benchmarks**		
41	Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Industry standards for service-level agreements may provide a reference point for standardized	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements.	Services

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.		
42	**Responsibilities for Providing, Receiving, and Retaining Information**		
43	Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. Stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.	Performance reports You can monitor Google's performance of the Services (including the SLAs) on a regular 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. • **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). Financial reports 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. Audit reports Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Refer to Row 16 for more information on the certifications and audit reports that Google maintains. You can review Google's current certifications and audit reports at any time. Business resumption testing reports Refer to row 56. 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 on our Incidents & the Google Cloud dashboard.	Ongoing Performance Monitoring Certifications and Audit Reports Significant Developments
44	Ensure that the contract sufficiently addresses	Termination	

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	• the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship. • the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions. • the bank's materiality thresholds and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the bank. • notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology. • notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved. • the ability of the third party to resell, assign, or permit access to the bank's data and systems to other entities. • the bank's obligations to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party.	Refer to row 66 Notification Refer to rows 24 and 70 Ownership Refer to row 52	
45	**The Right to Audit and Require Remediation**		
46	Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.	Performance monitoring Refer to row 43 for more information on how you can monitor Google's performance. Audit reports Refer to row 16 for more information on the audit reports that Google maintains. Audits Google recognizes that banks must be able to audit our services effectively. Google grants audit rights to banks and their representatives. The bank is best placed to decide what audit frequency is right for their organization. Our contract does not limit banks to a fixed number of audits.	Enabling Customer Compliance
47	**Responsibility for Compliance With Applicable Laws and Regulations**		
48	Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations. Ensure that the contract requires the third party to maintain policies and procedures which address the bank's right to conduct periodic reviews so as to verify the third party's compliance with the	Compliance Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services. Periodic reviews Refer to row 46 for more information on the audit rights Google grants to banks. Refer to row 43 for more information on how you can monitor Google's performance.	Representations and Warranties

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	bank's policies and expectations. Ensure that the contract states the bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and requires remediation if issues arise.		
49	**Cost and Compensation**		
50	Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Consider outlining cost and responsibility for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed, including limits on any cost increases.	Fees Refer to your Google Cloud Financial Services Contract. Audit Google is committed to supporting banks with audits or examinations 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 or examination. Google will provide further details of any fee in advance of the activity when the scope of the activity is known.	Payment Terms Enabling Customer Compliance; Fee
51	**Ownership and License**		
52	State whether and how the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material. Indicate whether any records generated by the third party become the bank's property. Include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).	Data You retain all intellectual property rights in your data, the data you derive from your data using our services, and your applications. Trademarks, logos etc Google will not use your brand features without your prior approval.	Intellectual Property Marketing and Publicity
53	**Confidentiality and Integrity**		
54	Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. Stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party. 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. Stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity.	Use of your 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. Security The security and privacy of information when using a cloud service consists of two key elements: 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. Refer to Row 18 for more information on Google's security practices.	Data Security; Security Measures (Data Processing and Security Terms)

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

		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 at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **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 at https://cloud.google.com/security/encryption-in-transit. (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 breaches 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.	Data Incidents (Data Processing and Security Terms)
55	**Business Resumption and Contingency Plans**		
56	Ensure the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and	Google will implement a disaster recovery and business contingency plan for our services, review and test it at least annually and ensure it remains current with industry standards. Banks can review our plan and testing results.	Business Continuity and Disaster Recovery

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

	equipment, and for maintaining current and sound business resumption and contingency plans. Include provisions—in the event of the third party's bankruptcy, business failure, or business interruption—for transferring the bank's accounts or activities to another third party without penalty. Ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements. Stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans.	In addition, information about how customers can use our Services in their own disaster recovery and business contingency planning is available in our Disaster Recovery Planning Guide.	
57	**Indemnification**		
58	Consider including indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.	Refer to your Google Cloud Financial Services Contract.	Indemnification
59	**Insurance**		
60	Stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.	Google will maintain insurance cover against a number of identified risks.	Insurance
61	**Dispute Resolution**		
62	Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period.	Refer to your Google Cloud Financial Services Contract.	Governing Law
63	**Limits on Liability**		
64	Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. Consider whether a contract would subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights.	Refer to your Google Cloud Financial Services Contract.	Liability
65	**Default and Termination**		
66	Ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination. Determine whether it includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship. Ensure the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense. Include termination and notification requirements with time frames	Termination Banks can elect to terminate our contract for convenience with advance notice, including if Google increases the fees or if necessary to comply with law. In addition, banks may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency.	Term and Termination

	to allow for the orderly conversion to another third party. Provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary. Clearly assign all costs and obligations associated with transition and termination.	Transfer Google recognizes that banks need sufficient time to exit our services (including to transfer services to another service provider). To help banks achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract. 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 and storage options on our Compute Engine Documentation page.	Transition Term Data Export (Data Processing and Security Terms)
67	**Customer Complaints**		
68	Specify whether the bank or third party is responsible for responding to customer complaints. If it is the third party's responsibility, specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank. The third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes.	Given the nature of the services, Google does not have direct interaction with the bank's customers.	N/A
69	**Subcontracting**		
70	Stipulate when and how the third party should notify the bank of its intent to use a subcontractor. Specify the activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors. Detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.	Google recognizes that banks 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. To enable banks to retain oversight of any subcontracting and provide choices about the	Google Subcontractors

OCC Third Party Risk Management Guidance (Bulletin 2013-29)

Google Cloud Platform Mapping

		services banks use, Google will: • provide information about our subcontractors (including their function and location); • provide advance notice of changes to our subcontractors; and • give banks the ability to terminate if they have concerns about a new subcontractor. Google will remain accountable to you for the performance of all subcontracted obligations.	
71	**Foreign-Based Third Parties**		
72	Include in contracts with foreign-based third parties choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of choice-of-law covenants, requirements on banks, protection of privacy of customer information, and the types of information that the third party or foreign governmental entities will provide upon request. Therefore, seek legal advice to ensure the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such arrangement.	Google LLC is the provider of the services for US-based institutions. 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
73	**OCC Supervision**		
74	In contracts with service providers, stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials. The OCC treats as subject to 12 USC 1867(c) and 12 USC 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.	Google grants audit, access and information rights to banks' regulatory agencies and their appointees.	Regulator Information, Audit and Access