Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

This document is designed to help state member banks, bank and savings and loan holding companies and U.S. operations of foreign banking organizations supervised by Reserve Banks (“**institutions**”) to consider the Board of Governors of the Federal Reserve System Guidance on Managing Outsourcing Risk dated 5 December 2013 (the “**Federal Reserve Guidance on Managing Outsourcing Risk**") in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on Section IV of the Federal Reserve Guidance on Managing Outsourcing Risk, on Service Provider Risk Management Programs, which includes: Due Diligence and Selection of Service Providers, Contract Provisions and Considerations, and Business Continuity and Contingency Considerations. For each paragraph of these Sections, we provide commentary to help you understand how you can address the Federal Reserve Guidance using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Federal Reserve Guidance on Managing Outsourcing Risk	Google Cloud Commentary	Google Cloud Financial Services Contract Reference
	IV. Service Provider Risk Management Programs		
1	**B. Due Diligence and Selection of Service Providers**		
	A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to: 1. Business background, reputation, and strategy; 2. Financial performance and condition; and 3. Operations and internal controls.	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
2	**1. Business Background, Reputation, and Strategy**		
3	Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees. The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services. Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.	Business background and strategy You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy and details of material pending legal proceedings. It also provides information about our organizational policies e.g. our Code of Conduct. Reputation • 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. • 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. • Performance record: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard.	N/A

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

4	**2. Financial Performance and Condition**		
5	Financial institutions should review the financial condition of the service provider and its closely-related affiliates. The financial review may include: •The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. •The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service. •The potential impact of the financial institution's business relationship on the service provider's financial condition. •The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract. •The adequacy of the service provider's insurance coverage. •The adequacy of the service provider's review of the financial condition of any subcontractors. •Other current issues the service provider may be facing that could affect future financial performance.	You can review information about Google's financial performance and condition on Alphabet's Investor Relations page. This provides information about our financial strength and sustainability, our areas of investment and growth as well as risk factors. Refer to row 17 on insurance and row 15 and 29 on subcontractors.	N/A
6	**3. Operations and Internal Controls**		
7	Financial institutions are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed: • Internal controls; • Facilities management (such as access requirements or sharing of facilities); • Training, including compliance training for staff; • Security of systems (for example, data and equipment); • Privacy protection of the financial institution's confidential information; • Maintenance and retention of records; • Business resumption and contingency planning; • Systems development and maintenance; • Service support and delivery; • Employee background checks; and • Adherence to applicable laws, regulations, and supervisory guidance.	Google recognizes that institutions need to review our operations and internal controls for the services 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) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports
8	**C. Contract Provisions and Considerations**		
9	Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service provider's strategy for providing those services will	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

	determine the terms of the contract. Elements of well-defined contracts and service agreements usually include:		
10	• **Scope**: Contracts should clearly define the rights and responsibilities of each party, including:		
11	o Support, maintenance, and customer service;	The support services are described on our technical support services guidelines page.	Technical Support
12	o Contract timeframes;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
13	o Compliance with applicable laws, regulations, and regulatory guidance;	Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services.	Representations and Warranties
14	o Training of financial institution employees;	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.	N/A
15	o The ability to subcontract services;	Google recognizes that institutions 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 ensure institutions 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 29.	Google Subcontractors
16	o The distribution of any required statements or disclosures to the financial institution's customers;	Given the nature of the services Google does not have direct interaction with the institution's customers.	N/A
17	o Insurance coverage requirements; and	Google will maintain insurance cover against a number of identified risks.	Insurance
18	o Terms governing the use of the financial institution's property, equipment, and staff.	Google doesn't make use of your physical property, equipment or staff to deliver our services. Refer to row 22 for Google's commitment about the use and protection of your data.	N/A
19	• **Cost and compensation**: Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of	Fees Refer to your Google Cloud Financial Services Contract. Audit Google is committed to supporting institutions 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	Payment Terms Enabling Customer Compliance; Fee

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

	variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.	provide further details of any fee in advance of the activity when the scope of the activity is known.	
20	• **Right to audit**: Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.	Audits Google recognizes that institutions must be able to audit our services effectively. Google grants audit rights to institutions and their representatives. The institution is best placed to decide what audit frequency is right for their organization. Our contract does not limit institutions to a fixed number of audits. Audit reports Refer to row 7 for more information on the audit reports that Google provides.	Enabling Customer Compliance Certifications and Audit Reports
21	• **Establishment and monitoring of performance standards**: Agreements should define measurable performance standards for the services or products being provided.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements.	Services
22	• **Confidentiality and security of information**: Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance[4] , as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers. Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.[5] If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy laws and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention. **Information security measures** The confidentiality and security 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. 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. Refer to 29. Your data and applications in the cloud	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

	When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.	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 **Use of your information** You can provide Google instructions about your data and Google will comply with those instructions. 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. **Privacy and NonPublic Personal Information**	

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

		The Cloud Data Processing Addendum addresses the roles and responsibilities of the parties for your data. In particular, Google will: • comply with privacy laws and regulations applicable to it in the provision of the Services. • 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. • enable you to delete your information and comply with your instruction to delete your information from Google's systems.	Google's Compliance with Instructions (Cloud Data Processing Addendum) Protection of Customer Data Processing of Data; Roles and Regulatory Compliance (Cloud Data Processing Addendum) Data Incidents (Cloud Data Processing Addendum)

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

			Data Deletion (Cloud Data Processing Addendum)
23	• **Ownership and license**: Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address ownership and control of any information generated by service providers. If financial institution purchase software from service providers, escrow agreements may be needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Refer to row 22 for Google's commitment about the use and protection of your data.	Intellectual Property
24	• **Indemnification**: Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.	Google provides institutions with an indemnity for certain third party claims.	Indemnification
25	• **Default and termination**: Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.	Termination Institutions 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, institutions 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. Transfer Google recognizes that institutions need sufficient time to exit our services (including to transfer services to another service provider). To help institutions 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.	Term and Termination Transition Term Data Export (Cloud Data Processing Addendum)

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

		Refer to row 22 for Google's commitment about deleting your data.	
26	• **Dispute resolution**: Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.	Refer to your Google Cloud Financial Services Contract.	Governing Law
27	• **Limits on liability**: Service providers may want to contractually limit their liability. The board of directors and senior management of a financial institution should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform. [9]	Refer to your Google Cloud Financial Services Contract.	Liability
28	• **Foreign-based service providers**: For agreements with foreign-based service providers, financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.	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
29	• **Subcontracting**: If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.	<u>Accountability and due diligence</u> 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 subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable. Google will remain accountable to you for the performance of all subcontracted obligations. <u>Information and changes</u> To enable institutions to retain oversight of any subcontracting and provide choices about the services institutions use, Google will: ● provide information about our subcontractors (including their function and location); ● provide advance notice of changes to our subcontractors; and ● give institutions the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
30	**F. Business Continuity and Contingency Considerations**		
31	Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans	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.	N/A

Federal Reserve Guidance on Managing Outsourcing Risk

Google Cloud Mapping

	during operational disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform." [11] When preparing contingency plans, financial institutions should:		
32	• Ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;	This is a customer consideration. Information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	N/A
33	• Assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;	Google will implement a business continuity plan for our services, review and test it at least annually and ensure it remains current with industry standards. Institutions can review our plan and testing results.	Business Continuity and Disaster Recovery
34	• Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;	Refer to row 33.	Refer to row 33.
35	• Test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and	Refer to row 33.	Refer to row 33.
36	• Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.	This is a customer consideration. Refer to row 25 for more information about how our Services support exit.	N/A