FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

This document is designed to help financial institutions (“**institutions**”) within the Federal Financial Institutions Examination Council’s (“**FFIEC**”) mandate to consider the Outsourcing Technology Services Booklet (the “**FFIEC Outsourcing Booklet**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the Due Diligence and Contract Issues sections of the FFIEC Outsourcing Booklet. For each paragraph of these sections, we provide commentary to help you understand how you can address the FFIEC Outsourcing Booklet using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Reference	Google Cloud Commentary	Google Cloud Financial Services Contract reference
1	**Due Diligence**		
2	A financial institution should perform due diligence on the service provider's response to an RFP as well as the service provider itself. Due diligence should serve as a verification and analysis tool, providing assurance that the service provider meets the institution's needs. Due diligence should confirm and assess the following information regarding the service provider:	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	• Existence and corporate history;	Information about Google Cloud’s corporate history is available on Alphabet’s Investor Relations page.	N/A
4	• Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate;	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
5	• Other companies using similar services from the provider that may be contacted for reference;	Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Customer page.	N/A
6	• Financial status, including reviews of audited financial statements;	You can review Google’s financial status and audited financial statements on Alphabet’s Investor Relations page.	N/A
7	• Strategy and reputation;	Strategy Information about Google Cloud’s strategies is available on Alphabet’s Investor Relations page. Reputation See how Google Workspace customers from a variety of industries have used Google Workspace to transform their businesses.	N/A
8	• Service delivery capability, status, and effectiveness;	Information about Google Cloud’s service delivery capability and effectiveness is available on our Choosing Google Cloud page. In addition, you can review reports by third party industry analysts on our Analyst Reports page.	N/A

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

9	• Technology and systems architecture;	Information about Google Cloud's technology and systems architecture is available on our Choosing Google Cloud page.	N/A
10	• Internal controls environment, security history, and audit coverage;	Google recognizes that institutions 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) • ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 • SOC 3	N/A
11	• Legal and regulatory compliance including any complaints, litigation, or regulatory actions;	Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
12	• Reliance on and success in dealing with third party service providers;	Refer to row 41 on subcontracting.	N/A
13	• Insurance coverage; and	Google will maintain insurance cover against a number of identified risks.	N/A
14	• Ability to meet disaster recovery and business continuity requirements.	Refer to row 40 on business resumption and contingency plans.	N/A
15	Other important elements include probing for information on intangibles, such as the third party's service philosophies, quality initiatives, and management style. The culture, values, and business styles should fit those of the financial institution.	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organizational policies e.g. our Code of Conduct.	N/A
16	When a foreign-based service provider is considered, the evaluation should assess the relationship in light of the above items as well as the information discussed in Appendix C, Foreign-Based Third-Party Service Providers.	Refer to row 50.	N/A
17	Financial institutions may perform due diligence on one or more of the service providers that respond to the RFP. The depth and formality of the due diligence performed may vary according to the risk of the outsourced relationship, the institution's familiarity with the prospective service providers, and the stage of the provider selection process. Once institutions issue RFPs, receive and evaluate responses, and perform due diligence, they enter into contract negotiations with one or more of the service providers they have determined can best meet their needs.	This is a customer consideration.	N/A
18	**Contract Issues**		
19	After selecting a service provider, management should negotiate a contract that meets their requirements. The RFP and the service provider's response can be used as inputs to this process. The contract is the legally binding document that defines all aspects of	The Google Cloud Financial Services Contract defines the aspects of the service relationship.	N/A

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

	the servicing relationship. A written contract should be present in all servicing relationships. This includes instances where the service provider is affiliated with the institution. When contracting with an affiliate, the institution should ensure the costs and quality of services provided are commensurate with those of a nonaffiliated provider. The contract is the single most important control in the outsourcing process. Because of the importance of the contract, management should: • Verify the accuracy of the description of the outsourcing relationship in the contract; • Ensure the contract is clearly written and contains sufficient detail to define the rights and responsibilities of each party comprehensively; and • Engage legal counsel early in the process to help prepare and review the proposed contract.		
20	Examples of contract elements that should be considered include:		
21	**Scope of Service**. The contract should clearly describe the rights and responsibilities of the parties to the contract. Considerations should include:	The rights and responsibilities obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
22	• Descriptions of required activities, timeframes for their implementation, and assignment of responsibilities. Implementation provisions should take into consideration other existing systems or interrelated systems to be developed by different service providers (e.g., an Internet banking system being integrated with existing core applications or systems customization);	Activities The Google Workspace services are described on our services summary page. Integration 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.	Definitions
23	• Obligations of, and services to be performed by, the service provider including software support and maintenance, training of employees, or customer service;	Google will provide the Services described on our services summary page in accordance with the Google Workspace Service Level Agreements. The support services are described on our Google Workspace technical support services guidelines page. Google provides documentation to explain how institutions and their employees can use our Google Workspace services. If an institution would like more guided training, Google also provides a variety of courses and certifications.	Services Technical Support
24	• Obligations of the financial institution;	Refer to your Google Cloud Financial Services Contract.	

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

25	• The contracting parties' rights in modifying existing services performed under the contract; and	Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
26	• Guidelines for adding new or different services and for contract re-negotiation.	New services Google is continuously introducing new services to offer our customers the latest features and functionality. New services are added to the services summary page when they are available and each customer can choose whether or not to use them under their existing contract. Contract re-negotiation As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties.	Updates to Services and Terms Changes to Terms; Amendments
27	**Performance Standards.** Institutions should include performance standards that define minimum service level requirements and remedies for failure to meet standards in the contract. For example, common service level metrics include percent system uptime, deadlines for completing batch processing, or number of processing errors. Industry standards for service levels may provide a reference point. The institution should periodically review overall performance standards to ensure consistency with its goals and objectives. Also see the Service Level Agreements section in this booklet.	The SLAs are available on our Google Workspace Service Level Agreement page.	Services
28	**Security and Confidentiality.** The contract should address the service provider's responsibility for security and confidentiality of the institution's resources (e.g., information, hardware). The agreement should prohibit the service provider and its agents from using or disclosing the institution's information, except as necessary to or consistent with providing the contracted services, and to protect against unauthorized use (e.g., disclosure of information to institution competitors). If the service provider receives nonpublic personal information regarding the institution's customers, the institution should verify that the service provider complies with all applicable requirements of the privacy regulations. Institutions should require the service provider to fully disclose breaches in security resulting in unauthorized intrusions into the service	**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	Data Security; Security Measures (Data Processing Amendment)

	provider that may materially affect the institution or its customers. The service provider should report to the institution when intrusions occur, the effect on the institution, and corrective action to respond to the intrusion, based on agreements between both parties.	for all our customers. This is described in the Data Processing Amendment. 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 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 certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data. at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. (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.	

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

		(c) Security resources Google also publishes guidance on: • Security best practices • Security use cases **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. **Privacy and Non-Public Personal Information** Google will comply with privacy laws and regulations applicable to it in the provision of the Services. **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.	Protection of Customer Data Processing of Data; Roles and Regulatory Compliance (Data Processing Amendment) Data Incidents (Data Processing Amendment)
29	**Controls**. Management should consider implementing contract provisions that address the following controls:		
30	• Service provider internal controls;	Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of the effectiveness of our internal controls. To give you visibility of the effectiveness of our internal controls throughout our relationship, Google commits to maintain certifications / reports for 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) • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports
31	• Compliance with applicable regulatory requirements;	Google will comply with all laws and regulations applicable to it in the provision of the Services.	Representations and Warranties
32	• Record maintenance requirements for the service provider;	Google grants access and information rights to institutions and their appointees.	Customer Information, Audit and Access

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

33	• Access to the records by the institution;	Refer to row 32	
34	• Notification requirements and approval rights for any material changes to services, systems, controls, key project personnel, and service locations;	<u>Services</u> Refer to row 25 on changes to the services. <u>Personnel</u> 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. <u>Locations</u> To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities is available here • Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data - including a choice to store your data in the United States. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy on Google Cloud Whitepaper.	Data Transfers (Data Processing Amendment) Data Security; Subprocessors (Data Processing Amendment) Data Location (Service Specific Terms)
35	• Setting and monitoring parameters for financial functions including payments processing or extensions of credit on behalf of the institution; and	Given the nature of the services, Google does not perform payment processing (in the sense intended in the Booklet) or extensions of credit on behalf of the institution.	N/A
36	• Insurance coverage maintained by the service provider.	Google will maintain insurance cover against a number of identified risks.	Insurance
37	**Audit**. The institution should include in the contract the types of audit reports it is entitled to receive (e.g., financial, internal control, and security reviews). The contract	<u>Audit reports</u>	Certifications and Audit Reports;

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

	should specify the audit frequency, any charges for obtaining the audits, as well as the rights of the institution and its regulatory agencies to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the processing facilities and operating practices of the service provider. Management should consider, based upon the risk assessment phase, if it can rely on internal audits or if there is a need for external audits and reviews.	Refer to row 10 for more information on the audit reports that Google provides. Google commits to maintain these reports throughout the term of our contract with you. The reports are produced on at least an annual basis after an audit by an independent third-party. You can review Google's current certifications and audit reports at any time. • Google's **ISO certifications** are available here. • Google's **SOC reports** and **PCI Attestation of Compliance (AOC)** are available via your Google Cloud account representative. Institutions may provide these materials to their regulatory agencies. Inspection Google recognizes that institutions must be able to audit our services effectively. Google grants audit rights to institutions and their independent auditors, including to inspect Google's processing facilities and operating practices. 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.	Enabling Customer Compliance
38	For services involving access to open networks, such as Internet-related services, management should pay special attention to security. The institution should consider including contract terms requiring periodic control reviews performed by an independent party with sufficient expertise. These reviews may include penetration testing, intrusion detection, reviews of firewall configuration, and other independent control reviews. The institution should receive sufficiently detailed reports on the findings of these ongoing audits to assess security adequately without compromising the service provider's security.	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
39	**Reports**. Contractual terms should include the frequency and type of reports the institution will receive (e.g., performance reports, control audits, financial statements, security, and business resumption testing reports). The contracts should also outline the guidelines and fees for obtaining custom 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. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.	Ongoing Performance Monitoring

		• Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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 As a subscription service, Google Workspace offers you the ability to choose the pricing structure that works best for your organization. Prices and fee information are publicly available on our Pricing page. You can also access our Google Workspace Admin Help page for comparing Google Workspace billing plans. Audit and security reports Refer to row 10. Business resumption testing reports Refer to row 40. 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 Google Workspace Status Dashboard.	Significant Developments
40	**Business Resumption and Contingency Plans**. The contract should address the service provider's responsibility for backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans. The contracts should outline the service provider's responsibility to test the plans regularly and provide the results to the institution. The institution should consider interdependencies among service providers when determining business resumption testing requirements. The service provider should provide the institution a copy of the contingency plan that outlines the required operating procedures in the event of business disruption. Contracts should include specific provisions for business recovery timeframes that meet the institution's business requirements. The institution should ensure that the contract does not contain any provisions that would excuse the service provider from implementing its contingency plans.	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. Institutions can review our plan and testing results. 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.	Business Continuity and Disaster Recovery
41	**Sub-contracting and Multiple Service Provider Relationships**. Some service providers may contract with third parties in providing services to the financial institution. Institutions should be aware of and approve all subcontractors. To provide accountability, the financial institution should designate the primary contracting service provider in the contract. The contract should also specify that the primary contracting service provider is responsible for the services outlined in the contract regardless of	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.	Google Subcontractors

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

	which entity actually conducts the operations. The institution should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.	Accountability 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. Google will remain responsible for the performance of all subcontracted obligations. Information and changes 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.	
42	**Cost.** The contract should fully describe the calculation of fees for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity or for special requests. Contracts should also address the responsibility and additional cost for purchasing and maintaining hardware and software. Any conditions under which the cost structure may be changed should be addressed in detail including limits on any cost increases. Also see the Pricing Methods and Bundling sections in this booklet.	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 provide further details of any fee in advance of the activity when the scope of the activity is known.	Payment Terms
43	**Ownership and License.** The contract should address the ownership, rights to, and allowable use of the institution's data, equipment/hardware, system documentation, system and application software, and other intellectual property rights. Ownership of the institution's data must rest clearly with the institution. Other intellectual property rights may include the institution's name and logo, its trademark or copyrighted material, domain names, web sites designs, and other work products developed by the service provider for the institution. Additional information regarding the development of customized software to support outsourced services can be found in the IT Handbook's "Development and Acquisition Booklet."	Data 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 28 for Google's commitment about the use and protection of your data. Trademarks, logos etc Google will not use your brand features without your prior approval.	Intellectual Property Marketing and Publicity
44	**Duration.** Institutions should consider the type of technology and current state of the industry when negotiating the appropriate length of the contract and its renewal periods. While there can be benefits to long-term technology contracts, certain technologies may be subject to rapid change and a shorter-term contract may prove beneficial. Similarly, institutions should consider the appropriate length of time required to notify the service provider of the institutions' intent not to renew the contract prior to expiration. Institutions should consider coordinating the expiration dates of contracts for	Refer to your Google Cloud Financial Services Contract.	Term and Termination

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

	inter-related services (e.g., web site, telecommunications, programming, network support) so that they coincide, where practical. Such coordination can minimize the risk of terminating a contract early and incurring penalties as a result of necessary termination of another related service contract.		
45	**Dispute Resolution**. The institution should consider including a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner as well as a provision for continuation of services during the dispute resolution period.	Refer to your Google Cloud Financial Services Contract.	Governing Law
46	**Indemnification.** Indemnification provisions should require the service provider to hold the financial institution harmless from liability for the negligence of the service provider. Legal counsel should review these provisions to ensure the institution will not be held liable for claims arising as a result of the negligence of the service provider.	Refer to your Google Cloud Financial Services Contract.	Indemnification
47	**Limitation of Liability.** Some service provider standard contracts may contain clauses limiting the amount of liability that can be incurred by the service provider. If the institution is considering such a contract, management should assess whether the damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the service provider's failure to perform its obligations.	Refer to your Google Cloud Financial Services Contract.	Liability
48	**Termination.** Management should assess the timeliness and expense of contract termination provisions. The extent and flexibility of termination rights can vary depending upon the service. Institutions should consider including termination rights for a variety of conditions including change in control (e.g., acquisitions and mergers), convenience, substantial increase in cost, repeated failure to meet service levels, failure to provide critical services, bankruptcy, company closure, and insolvency. The contract should establish notification and timeframe requirements and provide for the timely return of the institution's data and resources in a machine readable format upon termination. Any costs associated with conversion assistance should also be clearly stated.	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 the transition term. More information is available on our Google Account help page. • In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.	Term and Termination Transition Term Data Export (Data Processing Amendment)
49	**Assignment.** The institution should consider contract provisions that prohibit assignment of the contract to a third party without the institution's consent. Assignment provisions should also reflect notification requirements for any changes to material subcontractors.	Assignment Refer to your Google Cloud Financial Services Contract. Subcontracting	Assignment

FFIEC Risk Management for Outsourcing Technology Services

Google Workspace Mapping

		Refer to row 41 on subcontracting.	
50	**Foreign-based service providers.** Institutions entering into contracts with foreign-based service providers should consider a number of additional contract issues and provisions. See Appendix C included in this booklet.	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
51	**Regulatory Compliance.** Financial institutions should ensure that contracts with service providers include an agreement that the service provider and its services will comply with applicable regulatory guidance and requirements. The provision should also indicate that the service provider agrees to provide accurate information and timely access to the appropriate regulatory agencies based on the type and level of service it provides to the financial institution.	Compliance Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services. Access by regulatory agencies Google grants access and information rights to institutions' regulatory agencies and their appointees.	Representations and Warranties Regulator Information, Audit and Access