# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

This document is designed to help institutions supervised by the Federal Deposit Insurance Corporation (“**institutions**”) to consider Financial Institution Letter 44-2008 on Guidance for Managing Third Party Risk (the “**FDIC Guidance for Managing Third Party Risk**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the FDIC Guidance on Managing Third Party Risk: Section 2 on Due Diligence in Selecting a Third Party and Section 3 on Contract Structuring and Review. For each paragraph of these Sections, we provide commentary to help you understand how you can address the FDIC Guidanceusing the Google Cloud services and the Google Cloud Financial Services Contract.

| # | FDIC Guidance on Managing Third Party Risk | Google Cloud Commentary | Google Cloud Financial Services Contract Reference |
|---|---|---|---|
| | **Risk Management Process** | | |
| 1 | **2. Due Diligence in Selecting a Third Party** | | |
| 2 | Following an assessment of risks and a decision to proceed with a plan to establish a third-party relationship, management must select a qualified entity to implement the activity or program. The due diligence process provides management with the information needed to address qualitative and quantitative aspects of potential third parties to determine if a relationship would help achieve the financial institution's strategic and financial goals and mitigate identified risks. Not only should due diligence be performed prior to selecting a third party, but it should also be performed periodically during the course of the relationship, particularly when considering a renewal of a contract.<br><br>The scope and depth of due diligence is directly related to the importance and magnitude of the institution's relationship with the third party. For example, large-scale, highly visible programs or programs dealing with sensitive data integral to the institution's success warrant an in-depth due diligence of the potential third party, while the due diligence process for isolated low-risk third-party activities would be much less comprehensive.<br>Comprehensive due diligence involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls. The evaluation of a third party may include the following items: | 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 | • Audited financial statements, annual reports, SEC filings, and other available financial indicators. | You can review Google’s audited financial statements, annual reports and SEC filings on Alphabet’s Investor Relations page. | N/A |
| 4 | • Significance of the proposed contract on the third party's financial condition. | You can review information about Google’s financial condition on Alphabet’s Investor Relations page. | N/A |
| 5 | • Experience and ability in implementing and monitoring the proposed activity. | You can review information about Google’s historic performance of the services on our Google Cloud Status Dashboard. | N/A |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| 6 | • Business reputation. | 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. | N/A |
| 7 | • Qualifications and experience of the company's principals. | Information about Google Cloud's leadership team is available on our Media Resources page. | N/A |
| 8 | • Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies. | Information about Google Cloud's strategies, goals and initiatives as well as our organizational policies is available on Alphabet's Investor Relations page. | N/A |
| 9 | • Existence of any significant complaints or litigation, or regulatory actions against the company. | Information about material pending legal proceedings is available in our annual reports page | N/A |
| 10 | • Ability to perform the proposed functions using current systems or the need to make additional investment. | Refer to rows 4 to 8. | N/A |
| 11 | • Use of other parties or subcontractors by the third party. | Refer to row 29 on subcontractors. | N/A |
| 12 | • Scope of internal controls, systems and data security, privacy protections, and audit coverage. | **Controls, security and privacy**<br><br>The security and privacy of information when using a cloud service consists of two key elements:<br><br>Google's infrastructure<br><br>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.<br><br>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.<br><br>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.<br><br>More information is available at:<br><br>• Our infrastructure security page<br>• Our security whitepaper<br>• Our cloud-native security whitepaper<br>• Our infrastructure security design overview page<br>• Our security resources page<br><br>Your data and applications in the cloud<br><br>You define the security of your data and applications in the cloud. This refers to the | N/A |

| | | | |
|---|---|---|---|
| | | security measures that you choose to implement and operate when you use the Services.<br><br>(a) Security by default<br><br>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:<br><br>• **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.<br><br>• **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.<br><br>(b) Security products<br><br>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.<br><br>(c) Security resources<br><br>Google also publishes guidance on:<br><br>• Security best practices<br>• Security use cases<br><br>**Audit coverage**<br><br>Google recognizes that institutions need to review our internal controls, systems and data security and privacy protections 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:<br><br>• ISO/IEC 27001:2013 (Information Security Management Systems) | |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| | | • ISO/IEC 27017:2015 (Cloud Security)<br>• ISO/IEC 27018:2014 (Cloud Privacy)<br>• PCI DSS<br>• SOC 1<br>• SOC 2<br>• SOC 3 | |
| 13 | • Business resumption strategy and contingency plans. | Refer to row 38 on Google's business resumption and contingency plans. | N/A |
| 14 | • Knowledge of relevant consumer protection and civil rights laws and regulations. | Refer to row 24. | N/A |
| 15 | • Adequacy of management information systems. | Refer to row 34 on reports. | N/A |
| 16 | • Insurance coverage. | Refer to row 27 on insurance. | N/A |
| 17 | **3. Contract Structuring and Review** | | |
| 18 | After selecting a third party, management should ensure that the specific expectations and obligations of both the financial institution and the third party are outlined in a written contract prior to entering into the arrangement. Board approval should be obtained prior to entering into any material third-party arrangements. Appropriate legal counsel should also review significant contracts prior to finalization. Any material or significant contract with a third party should prohibit assignment, transfer or subcontracting by the third party of its obligations to another entity, unless and until the financial institution determines that such assignment, transfer, or subcontract would be consistent with the due diligence standards for selection of third parties. | Assignment<br>Refer to your Google Cloud Financial Services Contract.<br><br>Subcontracting<br>Refer to row 29 on subcontracting. | Assignment |
| 19 | The level of detail in contract provisions will vary with the scope and risks associated with the third-party relationship. The following topics should be considered as a contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship. | | |
| 20 | **Scope.** The contract should clearly set forth the rights and responsibilities of each party to the contract, including the following: | The rights and responsibilities obligations of the parties are set out in the Google Cloud Financial Services Contract. | N/A |
| 21 | • Timeframe covered by the contract. | Refer to your Google Cloud Financial Services Contract. | Term and Termination |
| 22 | • Frequency, format, and specifications of the service or product to be provided. | The GCP services are described on our services summary page. | Definitions |
| 23 | • Other services to be provided by the third party, such as software support and maintenance, training of employees, and customer service. | The support services are described on our technical support services guidelines page. | Technical Support |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| | | 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. | |
| 24 | • Requirement that the third party comply with all 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 |
| 25 | • Authorization for the institution and the appropriate federal and state regulatory agency to have access to records of the third party as are necessary or appropriate to evaluate compliance with laws, rules, and regulations. | Google grants access and information rights to institutions, regulatory agencies and both their appointees. | Regulator Information, Audit and Access; Customer Information, Audit and Access |
| 26 | • Identification of which party will be responsible for delivering any required customer disclosures. | Given the nature of the services Google does not have direct interaction with the institution's customers. | N/A |
| 27 | • Insurance coverage to be maintained by the third party. | Google will maintain insurance cover against a number of identified risks. | Insurance |
| 28 | • Terms relating to any use of bank premises, equipment, or employees. | Google doesn't make use of your premises, equipment or employees to deliver our services. | N/A |
| 29 | • Permissibility/prohibition of the third party to subcontract or use another party to meet its obligations with respect to the contract, and any notice/approval requirements. | 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.<br><br>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.<br><br>To enable institutions to retain oversight of any subcontracting and provide choices about the services institutions use, Google will:<br><br>• provide information about our subcontractors (including their function and location);<br>• provide advance notice of changes to our subcontractors; and<br>• give institutions the ability to terminate if they have concerns about a new subcontractor.<br><br>Google will remain accountable to you for the performance of all subcontracted obligations. | Google Subcontractors |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| 30 | • Authorization for the institution to monitor and periodically review the third party for compliance with its agreement. | You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.<br><br>For example:<br><br>• The **Status Dashboard** provides status information on the Services.<br><br>• **Google Stackdriver** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP.<br><br>• **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). | Ongoing Performance Monitoring |
| 31 | • Indemnification. | Refer to row 42 on indemnification. | Refer to row 42 |
| 32 | **Cost/compensation.** For both the financial institution and the third party, the contract should outline the fees to be paid, including any fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests. Other items that should be addressed, if applicable, are the cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other item related to the activity. Also, the party responsible for payment of any legal or audit expenses should be identified.<br><br>Financial institutions should employ compensation programs that are consistent with sound banking practices and consumer protection laws. Compensation schemes should be structured to promote favorable long-term performance in a safe and sound manner. Volume and short-term incentives should be subject to strict quality control, and in the area of loan originations, are of particular concern. The FDIC expressly discourages the use of compensation arrangements which may encourage third-party originators to inappropriately steer borrowers into higher cost products. | Fees<br>Refer to your Google Cloud Financial Services Contract.<br><br>Audit<br>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<br><br>Enabling Customer Compliance; Fee |
| 33 | **Performance standards.** For certain relationships, clearly defined performance standards should be included to serve as a basis for measuring the performance of the third party, and may also be used as a factor in compensation arrangements. Industry standards may be used as a reference for certain functions, or standards may be set to reflect the particular relationship between the third party and the financial institution. Management should periodically review the performance measures to ensure consistency with its overall objectives. | The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements. | Services |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| 34 | **Reports.** The contract should specify the type and frequency of management information reports to be received from the third party. Routine reports may include performance reports, audits, financial reports, security reports, and business resumption testing reports. Management should also consider mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the financial institution. | Performance reports<br>Refer to row 33.<br><br>Financial reports<br>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.<br><br>Audit and security reports<br>Refer to row 12.<br><br>Business resumption testing reports<br>Refer to row 38.<br><br>Exception-based reports<br>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 . | Significant Developments |
| 35 | **Audit.** In addition to the types and frequency of audit reports that the financial institution is entitled to receive from the third party, the contract should also specify the institution's right to audit the third party (or engage an independent auditor) as needed to monitor performance under the contract. Management should ensure that the third party's internal control environment as it relates to the service or product being provided to the financial institution is sufficiently audited. If material to the arrangement, specific internal controls to be maintained by the third party should be defined in the contract. | Audit reports<br>Refer to row 12 for more information on the audit reports that Google provides.<br><br>Audit<br>Google recognizes that institutions must be able to audit our services effectively. Google grants audit rights to institutions and their independent auditors. 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 |
| 36 | **Confidentiality and security.** The contract should prohibit the third party and its agents from using or disclosing the institution's information, except as necessary to perform the functions designated by the contract. Any nonpublic personal information on the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. Any breaches in the security and confidentiality of information, including a potential breach resulting from an unauthorized intrusion, should be required to be fully and promptly disclosed to the financial institution. | Use of your information<br>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.<br><br>Privacy and Non-Public Personal Information<br>Google will comply with privacy laws and regulations applicable to it in the provision of the Services.<br><br>Security breaches<br>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<br><br>Processing of Data; Roles and Regulatory Compliance (Cloud Data Processing Addendum)<br><br>Data Incidents (Cloud Data Processing Addendum) |
| 37 | **Customer complaints.** The contract should specify whether the financial institution or the third party has the duty to respond to any complaints received by the third party from | Given the nature of the services, Google does not have direct interaction with the institution's customers. | N/A |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| | customers of the financial institution. If the third party is responsible for such responses, a copy of any complaint and the response should be forwarded to the financial institution. The contract should also provide for periodic summary reports detailing the status and resolution of complaints. | | |
| 38 | **Business resumption and contingency plans.** The contract should address the third party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters. The third party should have appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. Results of testing of these plans should be provided to the financial institution. | 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.<br><br>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 |
| 39 | **Default and termination.** To mitigate risks associated with contract default and/or termination, the contract should address both issues. The contract should specify what circumstances constitute default, identify remedies, and allow for a reasonable opportunity to cure a default. Similarly, termination rights should be identified in the contract, especially for material third-party arrangements and relationships involving rapidly changing technology or circumstances. Termination rights may be sought for various conditions, such as a change in control, substantial increase in cost, failure to meet performance standards, failure to fulfill contractual obligations, inability to prevent violations of law, bankruptcy, company closure, and insolvency. The contract should state termination and notification requirements, with operating requirements and time frames to allow for the orderly conversion to another entity without excessive expense. Return of the financial institution's data, records, and/or other resources should also be addressed. | Termination<br>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.<br><br>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.<br><br>Transfer<br>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.<br><br>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:<br><br>• **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.<br><br>• **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine.<br><br>• 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<br><br>Transition Term<br><br>Data Export (Cloud Data Processing Addendum) |

# FDIC Guidance for Managing Third Party Risk (FIL-44-2008)

## Google Cloud Mapping

| | | | |
|---|---|---|---|
| 40 | **Dispute resolution.** The institution should consider whether the contract should include a dispute resolution process for the purpose of resolving problems expeditiously. Continuation of the arrangement between the parties during the dispute should also be addressed. | Refer to your Google Cloud Financial Services Contract. | Governing Law |
| 41 | **Ownership and license.** The contract should address ownership issues and the third party's right to use the financial institution's property, including data, equipment, software, and intellectual property such as the institution's name and logo, trademark, and other copyrighted material. It should also address ownership and control of any records generated by the third party. | Data<br>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 36 for Google's commitment about the use and protection of your data.<br><br>Trademarks, logos<br>Google will not use your brand features without your prior approval. | Intellectual Property<br><br>Marketing and Publicity |
| 42 | **Indemnification.** Indemnification provisions require a third party to hold the financial institution harmless from liability as a result of negligence by the third party, and vice versa. Incorporating these provisions into a contract may reduce the potential for the institution to be held liable for claims arising from the third party's negligence. It bears repeating, however, that such provisions cannot shift to third parties the institution's ultimate responsibility to conduct banking and related activities in a safe and sound manner and in compliance with laws, regulations and sound banking principles. Also, the existence of indemnification provisions will not be a mitigating factor where deficiencies indicate the need to seek corrective actions. Where violations of consumer protection or other laws, regulations, and sound banking principles are present, or when banking and related activities are not conducted in a safe and sound manner, the FDIC's consideration of remedial measures, including restitution orders, will be made irrespective of the existence of indemnification clauses in third-party contracts. | Refer to your Google Cloud Financial Services Contract. | Indemnification |
| 43 | **Limits on liability.** A third party may wish to contractually limit the amount of liability that it could incur as a result of the relationship with the financial institution. Before entering into such a contract, management of the financial institution should carefully consider whether the proposed damage limitation is reasonable compared to the amount of loss the institution could experience should the third party fail to adequately perform. | Refer to your Google Cloud Financial Services Contract. | Liability |