



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

This document is designed to help federally regulated entities supervised by the Office of the Superintendent of Financial Institutions (“**regulated entity**”) to consider the [B-10 Outsourcing of Business Activities, Functions and Process](#) guideline (the “**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: 7. Risk Management Program for Material Outsourcing Arrangements, 7.1 Due Diligence Processes, 7.2 Policies and Procedures to Manage Risks Associated with Material Outsourcing Arrangements and Annex 3 Due Diligence of Service Providers. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
7. Risk Management Program for Material Outsourcing Arrangements			
1.	In general, OSFI expects that an FRE will design a risk management program that applies to all outsourcing arrangements of the FRE group, except those that are clearly immaterial, and that the risk mitigants employed will be commensurate with the FRE’s assessment of the risks associated with the particular outsourcing arrangement.	This is a customer consideration.	N/A
7.1 Due Diligence Processes			
2.	OSFI expects an FRE to conduct an internal due diligence to determine the nature and scope of the business activity to be outsourced, its relationship to the rest of the FRE’s activities, and how the activity is managed.	This is a customer consideration.	N/A
3.	In selecting a service provider, or substantially amending or renewing a contract or outsourcing agreement, FREs are expected to undertake a due diligence process that fully assesses the risks associated with the outsourcing arrangement, and addresses all relevant aspects of the service provider, including qualitative (i.e., operational) and quantitative (i.e., financial) factors (see Annex 3 for a list of factors that could be included when performing due diligence of a service provider). When out-of-Canada outsourcing is being contemplated, the FRE should pay particular attention to the legal requirements of that jurisdiction, as well as the potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider’s ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program.	<p><u>Due diligence</u></p> <p>Google recognizes that you need to perform a risk assessment before deciding to use our services. To assist you, we’ve provided information for each of the listed factors in Annex 3 that you need to consider in Rows 42 to 50.</p> <p><u>Foreign outsourcing</u></p> <p>For more information on where Google provides the Services and the choices you have about where you store your data, refer to Row 41.</p>	N/A
4.	Due diligence processes will vary depending on the FRE and on the nature of the outsourcing arrangement being contemplated. For example, in the case of renewals where no material change has occurred that would affect the viability of the outsourcing relationship, it may be appropriate to conduct more streamlined due diligence. If the service provider is a member of an RFIP Group, a streamlined due diligence process may be followed that addresses the qualitative aspects of the arrangement, particularly those pertaining to the unique operational (e.g., Canadian) requirements of the FRE.	This is a customer consideration.	N/A
5.	The FRE may rely on a due diligence review of the service provider that has been performed by an affiliate or home office within the previous 15 months, provided the review addresses the above-noted requirements as well as the risks particular to the FRE.	This is a customer consideration.	N/A
7.2 Policies and Procedures to Manage Risks Associated with Material Outsourcing Arrangements			
6.	7.2.1 Contract for Services		
7.	OSFI expects material outsourcing arrangements to be documented by a written contract that addresses all elements of the arrangement and has been reviewed by the	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	FRE's legal counsel. Some of the items identified below may not be applicable in all circumstances; however, FREs are expected to address all issues relevant to managing the risks associated with each outsourcing arrangement to the extent feasible and reasonable given the circumstances, and having regard to the interests of the FRE. FRE and RFIP intra-group outsourcing arrangements can be documented by an outsourcing agreement that meets the expectations set out in Sections 4.1 and 4.2 respectively.		
8.	<i>a) Nature and Scope of the Service Being Provided</i>		
9.	The contract or outsourcing agreement is expected to specify the scope of the relationship, which may include provisions that address the frequency, content and format of the service being provided. The contract or outsourcing agreement is expected to detail the physical location where the service provider will provide the service.	<p><u>Scope of the relationship</u></p> <p>The GCP services are described on our services summary page.</p> <p><u>Locations</u></p> <p>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.</p> <ul style="list-style-type: none"> Information about the location of Google's facilities and where individual GCP services can be deployed is available here. Information about the location of Google's subprocessors' facilities is available here. 	<p>Definitions</p> <p>Data Transfers (Cloud Data Processing Addendum)</p>
10.	<i>b) Performance Measures</i>		
11.	Performance measures should be established that allow each party to determine whether the commitments contained in the contract are being fulfilled.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements .	Services
12.	<i>c) Reporting Requirements</i>		
13.	The contract or outsourcing agreement is expected to specify the type and frequency of information the FRE receives from the service provider. This would include reports that allow the FRE to assess whether the performance measures are being met and any other information required for the FRE's monitoring program (see Section 7.3). In addition, the contract or outsourcing agreement is expected to include procedures and requirements for the service provider to report events to the FRE that may have the potential to materially affect the delivery of the service.	<p><u>Monitoring</u></p> <p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <ul style="list-style-type: none"> The Status Dashboard provides status information on the Services. Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. 	Ongoing Performance Monitoring



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> 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). <p><u>Reporting</u></p> <p>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 page.</p> <p>In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.</p>	<p>Significant Developments</p> <p>Data Incidents (Cloud Data Processing Addendum)</p>
14.	<i>d) Resolution of Differences</i>		
15.	OSFI expects the contract or outsourcing agreement to incorporate a protocol for resolving disputes. The contract or outsourcing agreement should specify whether the service provider must continue providing the service during a dispute and the resolution period, as well as the jurisdiction and rules under which the dispute will be settled.	Refer to your Google Cloud Financial Services Contract.	Governing Law
16.	<i>e) Defaults and Termination</i>		
17.	The contract or outsourcing agreement is expected to specify what constitutes a default, identify remedies, and allow for opportunities to cure defaults or terminate the agreement. The FRE is expected to ensure that it can reasonably continue to process information and sustain operations in the event that the outsourcing arrangement is terminated or the service provider is unable to supply the service. Appropriate notice should be required for termination of service and the FRE's assets should be returned in a timely fashion. In particular, data and records relating to data processing outsourcing arrangements should be returned to the FRE in a format that would allow the FRE to sustain business operations without prohibitive expense.	<p><u>Remedies</u></p> <p>If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.</p> <p><u>Termination</u></p> <p>Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.</p>	<p>Services</p> <p>Term and Termination</p>



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p><u>Deletion</u></p> <p>On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.</p> <p><u>Return of data</u></p> <p>Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 	<p>Deletion on Termination (Cloud Data Processing Addendum)</p> <p>Transition Term</p> <p>Data Export (Cloud Data Processing Addendum)</p>
18.	The contract or outsourcing agreement should not contain wording that precludes the service from being continued in situations where the Superintendent takes control of the FRE, or where the FRE is in liquidation.	Google recognizes that regulated entities must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution as required.	Support through Resolution
19.	f) Ownership and Access		



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
20.	Identification and ownership of all assets (intellectual and physical) related to the outsourcing arrangement should be clearly established, including assets generated or purchased pursuant to the outsourcing arrangement. The contract or outsourcing agreement should state whether and how the service provider has the right to use the FRE's assets (e.g., data, hardware and software, system documentation or intellectual property) and the FRE's right of access to those assets.	<p><u>Data</u></p> <p>You retain all intellectual property rights in your data, the data you derive from your data using our services, and your applications. You may access your data at any time.</p> <p><u>Use of your information</u></p> <p>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.</p>	<p>Intellectual Property</p> <p>Protection of Customer Data</p>
21.	<i>g) Contingency Planning</i>		
22.	The contract or outsourcing agreement should outline the service provider's measures for ensuring the continuation of the outsourced business activity in the event of problems and events that may affect the service provider's operation, including systems breakdown and natural disaster, and other reasonably foreseeable events. The FRE should ensure that the service provider regularly tests its business recovery system as it pertains to the outsourced activity, notifies the FRE of the test results, and addresses any material deficiencies. The FRE is expected to provide a summary of the test results to OSFI upon reasonable notice. In addition, the FRE should be notified in the event that the service provider makes significant changes to its business resumption and contingency plans, or encounters other circumstances that might have a serious impact on the service.	<p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> <p>For more information on how Google notifies regulated entities of circumstances that have a serious impact on the services, refer to Row 13.</p>	Business Continuity and Disaster Recovery
23.	<i>h) Audit Rights</i>		
24.	The contract or outsourcing agreement is expected to clearly stipulate the audit requirements and rights of both the service provider and the FRE. At a minimum, it should give the FRE the right to evaluate the service provided or, alternatively to cause an independent auditor to evaluate, on its behalf, the service provided. This includes a review of the service provider's internal control environment as it relates to the service being provided.	<p>Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and their appointees. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.</p> <p>In addition, Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none"> • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) 	Customer Information, Audit and Access; Certifications and Audit Reports



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> • PCI DSS • SOC 1 • SOC 2 <p>You can review Google's current certifications and audit reports at any time.</p>	
25.	<p>In addition, in all situations, irrespective of whether an activity is conducted in-house, outsourced, or otherwise obtained from a third party, OSFI retains its supervisory powers. Accordingly, an undertaking from the service provider or a provision in the outsourcing contract, should give OSFI or the Superintendent's representative the right to:</p> <ul style="list-style-type: none"> • exercise the contractual rights of the FRE relating to audit; • accompany the FRE (or its independent auditor) when it exercises its contractual audit rights; • access and make copies of any internal audit reports (and associated working papers and recommendations) prepared by or for the service provider in respect of the service being performed for the FRE, subject to OSFI agreeing to sign appropriate confidentiality documentation in form and content satisfactory to the service provider; and • access findings in the external audit of the service provider (and associated working papers and recommendations) that address the service being performed for the FRE, subject to the consent of the service provider's external auditor and OSFI agreeing to sign appropriate confidentiality documentation in form and content satisfactory to the service provider and the external auditor. 	<p>Google recognizes that using our Services should not impair the supervisory authority's ability to supervise compliance with applicable laws and regulations. We will provide supervisory authorities with the assistance they need to review our Services.</p> <p>Google grants the same audit, access and information rights to supervisory authorities and their appointees as we grant to regulated entities. Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.</p>	Enabling Customer Compliance; Regulator Information, Audit and Access
26.	OSFI would provide the FRE with reasonable notice of its intent to exercise its audit rights and would share its findings with the FRE where appropriate. In the normal course, OSFI would seek to obtain information it requires through the FRE itself.	Reasonable notice enables Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer. Google recognizes that in some cases extended notice is not possible. In these cases we will work with the auditing party to address their needs.	Arrangements
27.	i) Subcontracting		
28.	The contract or outsourcing agreement is expected to set out any rules or limitations to subcontracting by the service provider. In particular, security and confidentiality standards should apply to subcontracting or outsourcing arrangements by the primary service provider. Consistent with the principles of this Guideline, the audit and inspection rights of the FRE and OSFI should continue to apply to all significant subcontracting arrangements.	<p>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:</p> <ul style="list-style-type: none"> • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new 	Google Subcontractors



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>subcontractor.</p> <p>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and inspection rights, and security requirements).</p>	
29.	j) Confidentiality, Security and Separation of Property		
30.	<p>At a minimum, the contract or outsourcing agreement is expected to set out the FRE's requirements for confidentiality and security. Ideally, the security and confidentiality policies adopted by the service provider would be commensurate with those of the FRE and should meet a reasonable standard in the circumstances. The contract or outsourcing agreement should address which party has responsibility for protection mechanisms, the scope of the information to be protected, the powers of each party to change security procedures and requirements, which party may be liable for any losses that might result from a security breach, and notification requirements if there is a breach of security.</p>	<p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security procedures and requirements and changes thereto as well as breaches.</p> <p>The confidentiality and security of a cloud service consists of two key elements:</p> <p><u>(1) Security of Google's infrastructure</u></p> <p>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p> <p>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.</p> <p>More information is available at:</p> <ul style="list-style-type: none"> • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page <p><u>(2) Security of your data and applications in the cloud</u></p> <p>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.</p> <p><u>(a) Security by default</u></p>	<p>Confidentiality</p> <p>Data Security; Security Measures (Cloud Data Processing Addendum)</p>



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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:</p> <ul style="list-style-type: none"> • 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. <p>(b) <u>Security products</u></p> <p>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.</p> <p>(c) <u>Security resources</u></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none"> • Security best practices • Security use cases 	
31.	OSFI expects appropriate security and data confidentiality protections to be in place. The service provider is expected to be able to logically isolate the FRE's data, records, and items in process from those of other clients at all times, including under adverse conditions.	To keep data private and secure, Google logically isolates each customer's data from that of other customers. For more information on Google's security infrastructure, refer to Row 30.	N/A
32.	k) Pricing		
33.	The contract or outsourcing agreement should fully describe the basis for calculating fees and compensation relating to the service being provided.	Refer to your Google Cloud Financial Services Contract.	Payment Terms
34.	l) Insurance		
35.	The service provider should be required to notify the FRE about significant changes in insurance coverage and disclose general terms and conditions of the insurance coverage.	Google will maintain insurance cover against a number of identified risks.	Insurance
36.	7.2.2 Location of Records		



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> Google makes the same commitments about all its subprocessors, regardless of country / region. <p>Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <p>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 for customers on Google Cloud Whitepaper.</p>	Data Transfers (Cloud Data Processing Addendum)
Annex 3 - Due Diligence of Service Providers			
42.	The due diligence of service providers addressed in Section 7.1 may include, but is not necessarily limited to, examining a service provider in light of these factors:	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 may need to consider in the rows that follow.	N/A
43.	Experience and technical competence of the service provider to implement and support the outsourced activity (this could include a review of the experience and technical competence of significant subcontractors where feasible);	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
44.	Financial strength (e.g., most recent audited financial statements and other relevant information (to the best of the service provider's ability));	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.	N/A
45.	Business reputation, complaints, compliance and pending litigation;	Customer references: Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. Information about material pending legal proceedings is available in our annual reports page	N/A
46.	Internal controls, reporting and monitoring environment;	<p>Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none"> 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 <p>You can review Google's current certifications and audit reports at any time.</p>	Certifications and Audit Reports



OSFI - B-10 Outsourcing Guidelines

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
47.	The service provider's business resumption and contingency measures, including recovery testing, for ensuring the continuation of the outsourced business activity in the event of problems and events that may affect the service provider's operation such as a systems breakdown, natural disaster, an inability of a significant subcontractor to provide services relevant to the outsourced activity, and situations where extraordinary demands are placed on a service provider	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.	Business Continuity and Disaster Recovery
48.	Reliance on and success in dealing with sub-contractors;	For more information on sub-contractors refer to Row 28.	N/A
49.	Insurance coverage; and	Google will maintain insurance cover against a number of identified risks.	Insurance
50.	Business objectives, human resource policies, service philosophies, business culture, and how they fit with those of the FRE.	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page.	N/A