ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

This document is designed to help financial entities supervised by the Autoridad de Supervisión del Sistema Financiero de Bolivia ("ASFI") ("**regulated entity**") to consider Title VII, Chapter II, "Information Security Management Regulation" ("**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: Section 11. Administration of Third Parties' Services and Contracts related with Information Technology. 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
1.	**CHAPTER II: INFORMATION SECURITY MANAGEMENT REGULATION**		
2.	**SECTION 11: ADMINISTRATION OF THIRD PARTIES' SERVICES AND CONTRACTS RELATED WITH INFORMATION TECHNOLOGY**		
3.	**Article 1. (Management of services and contracts with third parties)**		
4.	The Regulated Entity must have policies and procedures for the administration of services and contracts entered into with third parties in order to ensure that the contracted services are provided within the framework of an adequate level of services that minimize the related risk and are in accordance with the provisions contained in this Regulation as applicable. The General Management of the Regulated Entity must establish the responsibilities and procedures for the administration of the contracts and services entered into third parties.	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world. Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
5.	**Article 2. (Supplier Evaluation and Selection)**		
6.	For the hiring of information technology suppliers, the Regulated Entity must have a documented, formalized, updated, and implemented procedure; approved by the Board of Directors or equivalent body, to carry out the evaluation and selection of such suppliers prior to proceeding with their hiring.	Refer to Row 4.	N/A
7.	**Article 3. (Outsourced Data Processing or Systems Execution)**		
8.	For the hiring of companies responsible for data processing or systems execution at an external location, the Regulated Entity must consider at least the following aspects:	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
9.	a. It is the duty of the Board of Directors or equivalent body, General Management, and other responsible administrators to ensure that the supplier company has the necessary experience and capacity for processing data related to the business of the Regulated Entity and that they meet the characteristics of the service to be contracted;	Experience and capacity • 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. • Information about Google Cloud's leadership team is available on our Media Resources page. • Google Cloud has been providing cloud services for over 10 years, assisting	N/A

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

		customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. 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.	
10.	b. The technological infrastructure and systems used for communication, storage, and data processing must provide sufficient security to permanently protect the operational continuity, confidentiality, integrity, accuracy, and quality of the information and data. Additionally, it must be verified that they guarantee the timely acquisition of any necessary data or information to meet the purposes of the Regulated Entity or the requirements of competent authorities, such as the information that ASFI may request at any time.	Security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and integrity of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

		• Our security resources page (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
		Access to data	Regulator Information, Audit and Access

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

		You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access.	
11.	c. It is the responsibility of the Regulated Entity to verify and require the information technology supplier to comply with the relevant information security policies and procedures.	Refer to Row 10.	N/A
12.	d. It is the responsibility of the Regulated Entity to ensure the adoption of necessary measures that guarantee the operational continuity of data processing in the event of a change of external supplier or another unforeseen factor.	Change of supplier 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. Other factors 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.	Transition Term Business Continuity and Disaster Recovery
13.	e. In the event that data processing takes place outside of the national territory, the Regulated Entity must inform ASFI of this situation and attach the following documentation:	Locations 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. • Learn more about the location of Google's facilities and where individual GCP services can be deployed. • Learn more about the location of Google's subprocessors' facilities. 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	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

		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 Location (Service Specific Terms)
14.	1. Details of the decentralized activities;	The GCP services are described on our services summary page.	Definitions
15.	2. Description of the processing environment;	Refer to Row 10.	N/A
16.	3. List of processing personnel;	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.	N/A
17.	4. Responsible parties for processing control;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control the Services: • Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources. • gcloud Command Tool: A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer's operating system. • Google APIs: Application programming interfaces which provide access to GCP.	Instructions
18.	5. Report from the General Manager, addressed to the Board of Directors or equivalent body, indicating compliance with the provisions in the preceding paragraphs.	This is a customer consideration.	N/A
19.	Such documentation must be kept up-to-date by the Regulated Entity and be made available to ASFI.	This is a customer consideration.	N/A
20.	f. The General Manager of the supervised entity must present to the Board of Directors or equivalent body, a report with the character of a sworn declaration endorsed by the Internal Auditor, detailing the data processing or system execution services in charge of third parties, indicating the name of each of its suppliers, until March 31st of each year. Furthermore, the mentioned report should specify that the services provided by the suppliers that do not have a license to operate granted by ASFI, comply with the	This is a customer consideration.	N/A

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

	information security criteria established in Article 4° of Section 1 of this Regulation. The aforementioned Report will remain in the Supervised Entity for presentation to ASFI, when it so requires.		
21.	**Article 4. (Agreement with external processing supplier)**		
22.	It is the responsibility of the Board of Directors or equivalent body and the General Management of the Regulated Entity to sign the (the) contract(s) with the (the) supplier company (s) of the processing services, which among other things must minimally specify the following:	The rights and responsibilities obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
23.	a. The nature and specifications of the contracted processing services;	The GCP services are described on our services summary page. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Definitions Services
24.	b. The responsibility assumed by the supplier company to maintain policies and procedures that ensure the security, confidentiality and privacy of the information, in accordance with Bolivian legislation, as well as to prevent losses, unavailability or deterioration of the same;	Security, confidentiality and privacy This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. For more information refer to Row 10. Losses, unavailability and deterioration 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. Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum) Business Continuity and Disaster Recovery

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

		article for information about how you can achieve your desired reliability outcomes for your applications	
25.	c. The responsibility assumed by the supplier company in case its systems are breached, whether by internal and/or external computer attacks, deficiencies in parameterization, configuration and/or validation routines embedded in the source code;	Data incidents 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. Vulnerabilities Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Refer to our security whitepaper for more information. Configuration There are a number of ways to perform effective access / configuration management using the services: Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.	Data Incidents (Cloud Data Processing Addendum) Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
26.	d. The power of the Regulated Entity to periodically evaluate the company providing the service, directly or through independent audits.	Direct audits Google recognizes that regulated entities and their supervisory authorities must be	Customer Information, Audit and Access

		able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. Independent audits 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: • 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 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
27.	The Regulated Entity must keep the documents and records of contracts signed with technology information service supplier companies at the disposal of ASFI.	This is a customer consideration.	N/A
38.	**Article 9. (Service level agreement)**		
39.	The Regulated Entity, prior to the hiring of a third-party information technology supplier, must establish an Agreement of Service Level (SLA), a document that will be part of the respective contract, in accordance with the results of its analysis and evaluation of risks in security information and with the criticality of your operations. The SLA parameters must refer to the type of service, support and customer assistance, provisions for security and data, system guarantees and response times, availability of the service or system, connectivity, fines for system failure and/or alternative lines for the service, as appropriate.	The SLAs are available on our Google Cloud Platform Service Level Agreements page.	Services
40.	**Article 10. (Cloud computing service)**		
41.	The Regulated Entity, prior to contracting cloud computing service(s), must request no objection to ASFI in a written form, attaching for evaluation the "Implementation of the cloud computing service project", which has to reflect minimally, compliance with the following aspects:	This is a customer consideration.	
42.	a. That the right to Reserved and Confidentiality established in the Article 472 of the Law No. 393 on Financial Services is not infringed,	Refer to Row 10 on security.	N/A

ASFI – Section 11 Administration of Third Parties' Services and Contracts related with information Technology

Google Cloud Mapping

43.	b. It is not between the Limitations and Prohibitions, established in parts II, III and IV of the Law No. 393 on Financial Services, referred to "Financial Services and System of Authorizations" that may carry out the institutions supervised by ASFI.	This is a customer consideration.	N/A
44.	c. That the service supplier fulfill the safety requirements provided under this Regulations. (safety requirements)	Refer to Row 10 on security.	N/A
45.	d. The service supplier must comply with the proper standards with the legal regulations and the Plurinational State of Bolivia legislation, with the possibility of being examined by ASFI and/or Bolivian external audit firms	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access
46.	e. In its analysis and evaluation of the risks in information security, the pertinence of the cloud computing services contracting must be justified	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A
47.	f. That the clauses of the contract contemplate the aspects indicated in subparagraph a, b, c and d of this article.	This is a customer consideration.	
48.	ASFI may object the implementation of the cloud computing service, if the presented project, fails to comply with what is indicated in subparagraphs a, b, c, d and f and/or considers insufficient analysis and evaluation of information security risks, in relation to the relevance of contracting the cloud computing service (subsection e). In order to carry out the evaluation of the project, the Supervised Entity must send attached to it, a copy of the draft contract, as well as other documentation that it deems relevant.	Where relevant, regulated entities may disclose a copy of the contract to their supervisory authority.	Enabling Customer Compliance; Information
49.	**Article 11. (Cloud data protection)**		
50.	The Regulated Entity must have policies and procedures in order to define the criteria that guarantee due treatment, protection and privacy of personal data when using computer services in the cloud, considering the national regulations currently in force and the international references in this matter.	The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment.	N/A

		In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud.	
51.	**Article 12. (Risk level of the cloud computing service)**		
52.	The Regulated Entity, before contracting cloud computing services, must carry out a diagnosis of the level of risk and the sensitivity of information and/or technological resources to be exposed, which must be contained in the "Implementation of the cloud computing service Project".	Refer to Row 46.	N/A