Superintendencia de Banca (Peru)

Google Cloud Mapping

This document is designed to help firms and companies supervised by the Superintendencia de Banca (“**regulated entity**”) to consider: SBS Resolution No. 272.-2017 (Integrated Risk Management Regulations), SBS Resolution No.2116-2009 (Operation Risk Management Regulations), SBS Resolution No. 504-2021 (Data Security and Cybersecurity Management Regulations) and Circular G-139-2009 (Guidelines for Business Continuity) (“**frameworks**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the frameworks: Article 36 of SBS Resolution No. 272-2017 (Integrated Risk Management Regulations), Article 14 of SBS Resolution No. 2116-2009 (Operation Risk Management Regulations), Articles 22 - 25 of SBS Resolution No. 504-2021 (Data Security and Cybersecurity Management Regulations) and Section 8.4 of Circular G-139-2009 (Guidelines for Business Continuity). 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	**SBS Resolution No. 272-2017 (Integrated Risk Management Regulations)**		
2	**Article 36. Goods and/or services provided by third parties**		
3	36.1 Risks associated with the delivery of goods and/or services provided by third parties shall be managed as part of the integrated risk management of the firm.	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
4	36.2 The firm shall be responsible for the results of the goods and/or services provided by third parties under subcontracting schemes.	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
5	36.3 The firm shall conduct an assessment of the risks associated with material services provided by third parties, whether or not under a subcontracting scheme. Such assessment shall be submitted to the board of directors for approval thereof.	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

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
6	36.4 For all material subcontracting, the contracts entered with the providers shall contain clauses which enable an appropriate performance review by the firms, the internal audit unit, the external auditing firm, and the Superintendence or any designees thereof.	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. Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	Regulator Information, Audit and Access; Customer Information, Audit and Access Google Subcontractors
7	36.5 Subcontracting of risk management functions is deemed material for the purposes of these Regulations.	This is a customer consideration	N/A
8	36.6 This Superintendence may set additional requirements for some specific goods and/or services provided by third parties.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance.	Enabling Customer Compliance
9	**SBS Resolution No. 2116-2009: Operational Risk Management Regulations.**		
10	**Article 14. Goods and/or services provided by third parties**		
11	The firm must have appropriated policies and procedures in place to manage risks associated with services provided by third parties, and keep a record thereof.	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.	N/A
12	The firm should implement a procedure to identify material providers, specifying those cases in which they are under a subcontracting scheme.	This is a customer consideration. You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose.	N/A
13	For material services, whether or not under a subcontracting scheme, and of subcontracted services, the firm must consider the following:		
14	a) Implement a process to select 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 the information below. • 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 our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are	N/A

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. • Information about Google Cloud's leadership team is available on our Media Resources page. • You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct.	
15	b) Have an agreement, which is to include service levels; set forth the responsibilities of the provider and of the firm clearly; set the jurisdiction that will prevail in the event of conflict between the parties; and include the required information security levels.	Service Levels The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Responsibilities of the parties The responsibilities of the parties are set out in the Google Cloud Financial Services Contract. Jurisdiction Refer to your Google Cloud Financial Services Contract for more information about the governing law and jurisdiction that applies to our contract. Security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Services N/A Governing Law Data Security; Google's Security Measures (Cloud Data Processing Addendum)
16	c) Manage and monitor the risks associated with these services.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • 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, including availability and uptime of the services.	Ongoing Performance Monitoring

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **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).	
17	d) Keep a record containing at least the following:		
18	i) Name of the provider	Refer to our Google Contracting Entity page for information about which Google entity is the provider of the services in each country / region	N/A
19	ii) Line of business or core business of the provider	GCP is a public cloud service.	N/A
20	iii) Description or listing of services provides	The GCP services are described on our services summary page.	Definitions
21	iv) Countries, regions and/or geographical area where the contracted service is to be provided.	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 and where individual GCP services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. 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. 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 for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
22	v) Service levels agreed for the provision thereof	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
23	iii) Whether or not the subcontracting is deemed material by the firm	This is a customer consideration	N/A

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24	iv) Date of start of the service	Refer to your Google Cloud Financial Services Contract.	Term and Termination
25	v) Date of last renewal, if applicable	Refer to your Google Cloud Financial Services Contract.	Term and Termination
26	vi) Date when the service is due or next date of renewal of the contract, as applicable.	Refer to your Google Cloud Financial Services Contract.	Term and Termination
27	**Circular G-139-2009 (Guidelines for Business Continuity)**		
28	**8.4. Testing and Updating**		
29	Business continuity plans should be tested at least once a year. The following are the minimum activities that should be applied in this phase:	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. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
30	a. Test Performance: The scope of the tests should be consistent with the scope of the business continuity plans. Each test should have defined objectives and a report summarizing the results achieved and recommendations. This information should be used to improve business continuity plans in a timely manner. Different types of tests can be applied, from desk checks to full simulations of business interruption scenarios. Companies should ensure that their main service providers have continuity plans in place and that they comply with the provisions of this numeral.	See above. Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware.	Business Continuity and Disaster Recovery
31	b. Updating of Plans: Companies should define policies and procedures for updating business continuity management plans so that any changes that impact the company (whether internal or external) are reviewed in relation to business continuity.	This is a customer consideration.	N/A
32	**Resolution SBS No. 504-2021 (Data Security and Cybersecurity Management Regulations) - Chapter IV**		
33	**Article 22. Services rendered by Third Parties**		
34	In the case of services provided by third parties in aspects referring to information technology management, information security management or data processing, the company, in addition to complying with the requirements set forth in the Corporate Governance and Comprehensive Risk Management Regulations and the Regulations for Operational Risk Management must:	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and security of information when using 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.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page In addition, you can review Google's SOC 2 report. (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 on the Google Cloud Encryption at rest page. ● 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 on the Google Cloud Encryption in transit page. (b) Security products	

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
35	a. assess information security threats and vulnerabilities in the provision of goods and services and implement processing measures.	See above	N/A
36	b. Ensure that the contractual arrangement with the provider and its implementation allow it to comply with the obligations set forth in these Regulations.	See above	N/A
37	c. Establish the roles and responsibilities that the provider contractually assumes regarding information security and ensure that the company carries out the corresponding complementary implementations to meet the requirements of these Regulations.	See above	N/A
38	**Article 23. Use of Cloud Services:**		
39	In order to make use of cloud services, the company must implement information security policies and procedures that are of specific application, that take into account a framework of international good practices for the use of these services, and that in addition to the requirements of article 22 of the Regulations, include the following aspects:		
40	a. Information security requirements that cloud services must meet and procedures to ensure implementation prior to use.	Refer to Row 34 on Google's security practices.	N/A
41	b. Guidelines for network segregation that allow the isolation of the company's information from that of third parties in the shared environment of the cloud service.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
42	c. Evaluation of the availability of event logging offered by the cloud service provider and attention to the need for additional logs for information security monitoring.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example:	Ongoing Performance Monitoring

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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, including availability and uptime of the services. • **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). In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Autonomic Security Operations (ASO) solution: • delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. • enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. Here are some examples: • **Cloud Security Scanner** automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. • **Event Threat Detection** automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. • **Cloud Security Command Center** and **Security Health Analytics** provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
43	d. Provision of a training plan for management levels, administrators of these services, personnel in charge of their implementation and those who make use of them, on what is necessary for the management of information security in these services.	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	N/A
44	**Article 24. Significant Data Processing Services**		
45	24.1 The contracting of a significant service provided by third parties for data processing, including cloud services, must be considered as an important change in the IT environment, being applicable the definition of significant service established in the Corporate Governance and Comprehensive Risk Management Regulations and the regulations in force associated to new products and important changes.	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.	N/A
46	24.2 The company must comply with the following aspects referring to the contracting of a significant service provided by third parties for data processing, which includes cloud services, in a complementary manner to the provisions of Articles 22 and 23 of these Regulations, as applicable:		
47	a.Ensure adequate access to information, within reasonable times and upon request, by the Superintendence, Internal Audit and the External Audit Firm, under normal operating conditions and under special regimes.	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 Customer Information, Audit and Access
48	b. Manage Information security Incidents, in accordance with number 6 of Article 12, and to develop the planned activities provided for in Article 13 of these Regulations, as applicable to the significant data processing service in question.	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.	Data Incidents (Cloud Data Processing Addendum)
49	c. Have an exit strategy for the services provided by the provider that allows resuming operations on its own account or through another provider. Said strategy must foresee, among other aspects, the necessary actions for the migration of the information to the company's resources or to those of another provider.	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information. Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. 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.	Transition Term Data Export (Cloud Data Processing Addendum)

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	
50	d. Maintain an inventory of the services that the provider, in turn, contracts with third parties (chain contracting) and that are related to the services contracted by the company.	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • 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 subcontractor.	Google Subcontractors
51	e.Ensure that confidential information in the provider's custody is permanently deleted upon termination of the contractual agreement.	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
52	f. Verify annually that the data processing service provider has information security controls in place, in accordance with current information security regulations, as applicable to the service provided. This may be supported by independent reports and audit reports that include the verification of such controls in their scope.	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 • SOC 3 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

SBS - Outsourcing Resolutions

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
53	g. In the case of cloud services, in order to comply with the requirements of the previous letter, the company must annually prove that the provider maintains the ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 certifications in force, and that it has a SOC 2 type 2 report or other equivalents, relevant to the service provided and to the area or region from where the service is provided.	See above. Google facilities across the globe are included in the scope of our certifications and audit reports. Refer to the relevant certification or audit report for information about in scope locations.	N/A
54	24.3 The company must inform this Superintendence about the contracted service, the provider involved, the agreed service levels, the technological infrastructure used, as well as the procedures and responsible parties to comply with letters a) to 0, and as applicable g) of the previous paragraph; at the latest thirty (30) calendar days after starting the provision of data processing	This is a customer consideration.	M/A
55	**Article 25. Authorization for the Contracting of Significant Data Processing Services provided by Third Parties Abroad.**		
56	25.1 The company must request authorization from the Superintendence, prior to contracting a significant data processing service provided by third parties from abroad, in case said service has limitations to comply with the requirements established in paragraph 24.2 of article 24 of these Regulations, which shall be answered by the Superintendence within sixty (60) business days. In order to request such authorization, companies must submit, together with their request, a report with the legal grounds for the limitations identified and a proposed implementation plan for the compensatory measures.	Refer to Rows 45 to 54	N/A
57	25.2 The authorization granted by this Superintendence is specific to the service provider and to the country and city from which it is received, as well as to the general conditions that were the subject matter of the authorization; therefore, if there are modifications therein and if the limitation mentioned in the previous paragraph is maintained, a new authorization procedure before the Superintendence is required.	This is a customer consideration.	N/A