Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

This document is designed to help financial entities supervised by the Central Bank of the Argentine Republic (BCRA) ("**regulated entity**") to consider BCRA Comunicacion A 6375 (the "**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on Article 7.7 (Technical/Operational Requirements) of the framework. 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.	**7.7 Technical/Operational Requirements Tables**		
2.	**7.7.1 Information Security Governance.**		
3.	RGS001 - The entities/providers shall establish and inform to the BCRA a full, thorough, and updated detail of the shared and/or exclusive responsibilities of the roles and duties for the administration and operational management of information security related to the ITS.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security The security 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 ● Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud	Data Security; Security Measures (Cloud Data Processing Addendums)

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 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	
4.	RGS002 - The entity/provider shall establish the roles and duties for the treatment of customer data, setting forth the relevant responsibilities according to the level of participation and the task performed. These obligations shall be formally stated in the ITS agreements.	You operate the services independently without action by Google personnel. You decide which services to use, what information you provide and for what purpose. Therefore you stay in control of the treatment of your data.	Instructions

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
5.	RGS003 - The entity and the provider of the outsourced ITS shall comply with the domestic laws and regulations related to personal data protection (Act No. 25,326) whenever the service involves the collection and use of personal data, which should be reflected in the ITS agreements.	Google will comply with all national data protection regulations applicable to it in the provision of the Services.	Representations and Warranties
6.	RGS004 - The entity and the provider shall establish and document the protocols to exchange information among the parties to the ITS agreements, including subcontracted third parties, as well as the techniques and operational measures (formats, time frames, responsible individuals, etc.) that guarantee the provision of useful, timely, and full information to the parties involved and to the BCRA.	Information exchange You operate the services independently without action by Google personnel. You decide which services to use, what information you provide, and for what purpose. Refer to Row 4 for more information. Subcontractors Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. BCRA Regulated entities may provide their supervisory authority with access to their data on the services at their discretion.	Google Subcontractors Regulator Information, Audit and Access
7.	RGS005 - If the provider or subcontractors participating in an ITS process, store or transmit data or processes of the entity at sites located abroad, the entity, the providers and the third parties involved shall provide such mechanisms as may be necessary to verify if the relevant sites meet the legal, regulatory and contractual provisions set forth in the ITS agreement, including the terms in the rules on "Expansion of Financial Entities."	Location 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 here. ● Information about the location of Google's subprocessors' facilities is available here.	Data Transfers (Cloud Data Processing Addendum)

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. <u>Verification</u> 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 Google facilities across the globe are included in the scope of our certifications and audit reports. In addition, 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. These rights apply regardless of the service location.	Data Security; Subprocessors (Cloud Data Processing Addendum) Certifications and Audit Reports Customer Information, Audit and Access
8.	RGS006 - The ITS agreement shall include the obligation not to disclose personal data, which obligation shall be extended to subcontracted third parties.	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. Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and	Protection of Customer Data Requirements for Subprocessor Engagement (Cloud Data Processing Addendum)

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		to only access and use your data to the extent required to perform the obligations subcontracted to them.	
9.	RGS007 - The entities/providers shall document and assign the ownership of all the information assets in the ITS determining the level of administrative and operational responsibility of each party during the lifecycle of the information.	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. You operate the services independently without action by Google personnel. You decide which services to use, what information you provide and for what purpose. Therefore you stay in control of the treatment of your data. Google provides tools to help you manage your assets on our services. For example: • Cloud Asset Inventory allows you to view, monitor, and analyze all your GCP and Anthos assets across projects and services. Not only can you export a snapshot of your entire inventory at any point of time, you can also get real-time notifications on asset config changes. • Cloud Data Loss Prevention helps classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance.	Intellectual Property
10.	**7.7.2. Awareness and Training.**		
11.	RCC001 - The contents of the Awareness and Training (*Concientización y Capacitación*, CC) program shall be designed and kept updated based on an analysis of the vulnerabilities and the results of Incident Management, and they shall include, for example, reported, detected, and known incidents.	Security training All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Refer to our security whitepaper for more information. In addition, 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. Continuous improvement At Google, we strive to learn from every incident and implement preventative measures to avoid future incidents. The actionable insights from incident analysis enable us to	Personnel Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum) Data Incidents (Cloud Data Processing Addendum)

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		enhance our tools, trainings and processes, Google's overall security and privacy data protection program, security policies, and / or response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products. Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. Refer to our Data incident response whitepaper for more information.	
12.	RCC002 - The contents of the CC program shall include: techniques to detect and prevent the appropriation of personal data and credentials through "social engineering," "phishing," "vishing". and other similar attacks.	Refer to Row 11 for more information.	N/A
13.	RCC005 - To keep the internal staff, the staff responsible for the ITS management, the staff of third parties involved in operative tasks and customers informed about the communication channels that exist to receive reports or problems in the circuit related to the described scenario.	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. In addition, 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 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.	Data Incidents (Cloud Data Processing Addendum)
14.	RCC006- The following criteria must be applied with respect to the CC program audience:		

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
15.	a. Audience features and segmentation, according to the level of participation in the process and the nature of the duty or role of each participant.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
16.	b. All participants necessary to fully perform the activity stated in the scenario must be included.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
17.	c. Targeted at, but not limited to, the internal personnel, personnel responsible for the ITS management, suppliers, and customers.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
18.	RCC007 - The implemented CC program must be analyzed at least on an annual basis and such analysis shall measure the evolution of the incidents with respect to the CC activities, including, at least:		
19.	a. A report of the number and segmentation of intended recipients and contents of the CC program	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
20.	b. A comparison between the contents covered by the CC program and the quantity and type of reported/detected/known security incidents.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
21.	RCC008- The contents of the CC program must include: measures and techniques aimed at protecting the privacy of credentials.	Google shares best practices to help you manage your Google accounts. In addition, Google provides tools to help you secure your credentials. For example: Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud.	N/A
22.	RCC010 - The contents of the CC program must include: specific recommendations on security practices in the ITS support platform.	Google publishes a number of resources to help customers understand how to configure robust security for our services: • Security best practices • Security use cases • Security blueprints	N/A
23.	RCC012 - The contents of the CC program must include: specific techniques for the development/acquisition/manufacturing, implementation, validation and testing of the security features of the IT resources of the ITS ensuring that the internal/external personnel involved has been duly trained to reduce the implementation failures of the security features.	There are a number of ways to perform effective resource management using the services:	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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.	
24.	RCC013 - The entities/providers must have a mechanism to communicate the contents of their ITS awareness and training program that guarantees:		
25.	a. That the intended recipients are permanently informed.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
26.	b. That the intended recipients may make queries and resolve doubts.	This is a customer consideration. Refer to Rows 11 and 13 for information about how Google can support your awareness and training programs.	N/A
27.	**7.7.3. Access Control**		
28.	RCA049 - The entity and the provider shall ensure that personal data are not accessed/processed/exploited by them or any of their suppliers for purposes other than those established in the formal ITS agreements or without the formal and express consent of the party primarily responsible for the data.	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. Google also recognizes that you need visibility into who did what, when, and where for all user activity on our service. • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. • Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies.	Protection of Customer Data

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: • 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). • Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
29.	RCA050 - The entities/providers shall guarantee the entity and the BCRA unlimited access to all the documentation and information related to the ITS processing, operations, and procedures whenever such information is required.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities, supervisory authorities and both their appointees.	Customer Information, udit and Access Regulator Information, Audit and Access

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
30.	RCA051 - The entity shall guarantee that the ITS provider documents and supports the level of controls implemented to protect the services provided, through independent measures, external audits and certifications of international standards.	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
31.	RCA052 - The entities/providers shall have and implement an homogeneous policy for the administration of credentials, which will be based on the need of use/knowledge, the separation of incompatible roles and the prevention of collusions in order to have access to the following, among other things:		
32.	• Data encryption mechanisms and communication channels.	Refer to Row 28 for information on access management.	N/A
33.	• Privileged users of the operational/application platform.	Refer to Row 28 for information on access management.	N/A
34.	• Emergency/contingent users.	Refer to Row 28 for information on access management.	N/A
35.	• Regular users.	Refer to Row 28 for information on access management.	N/A
36.	Furthermore, they shall guarantee a lifecycle of the credentials, whose parameters, rules, algorithms, software components involved shall be updated and duly informed to the parties.	Refer to Row 28 for information on access management.	N/A
37.	**7.7.4. Integrity and Registration**		

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
38.	RIR003 - The records collected by the services provided by the provider shall guarantee the traceability of the actions performed with respect to all the activities, and they shall identify who (account, origin, destination), what (activity, function, transaction), where (service, location), when (time), how (pattern, relationship among events)	Refer to Row 28 for information about traceability. In addition, Cloud Audit Logs are encrypted at rest by default and reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. The service is also coupled with Google Cloud's Access Transparency service, which surfaces near real-time logs of GCP administrator access to your systems and data.	N/A
39.	RIR010 - The devices/equipment and/or software components provided by the entity/provider for the ITS must guarantee satisfaction of a lifecycle and a cycle of development, based on the following conceptual stages:		
40.	a. Analysis of requirements	Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. 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. Google's global scale infrastructure is designed to provide security through the entire information processing lifecycle. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Our infrastructure security page describes the security of this infrastructure in progressive layers starting from the physical security of our data centers, continuing on to how the hardware and software that underlie the infrastructure are secured, and finally, describing the technical constraints and processes in place to support operational security. Refer to Row 3 for more information about Google's security practices and the tools Google provides to help you monitor and enhance the security of your data.	Data Security; Security Measures (Cloud Data Processing Addendum)
41.	b. Acquisition/manufacturing/development.	Refer to row 40 for more information.	N/A
42.	c. Testing and validation.	Refer to row 40 for more information.	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
43.	d. Implementation.	Refer to row 40 for more information.	N/A
44.	e. Operation and maintenance.	Refer to row 40 for more information.	N/A
45.	f. Discard and replacement.	Refer to row 40 for more information.	N/A
46.	Furthermore, this cycle shall provide the security elements related, for example, to the following:		
47.	g. Functional security requirements.	Refer to Row 40 for information.	N/A
48.	h. Validation types and features of entry data.	Refer to Row 40 for information.	N/A
49.	i. Granularity of functions and records.	Refer to Row 40 for information.	N/A
50.	j. Levels of access.	Refer to Row 40 for information.	N/A
51.	k. Control of changes.	Refer to Row 40 for information.	N/A
52.	l. Updates and patches.	Refer to Row 40 for information.	N/A
53.	RIR011 - The entities/providers must run a validation process on the devices/equipment and/or software components to interact with the ITS guaranteeing the verification of all aspects of design, functionality, interoperability, and security features defined at the acquisition/manufacturing/development and implementation stages.	Refer to Row 40 for information.	N/A
54.	RIR020 - The entities/providers must have preventive and corrective mechanisms to handle the claims for access, modification and removal of personal data when requirements are made on the basis of the right of protection of the customer's data.	Refer to Row 28 for more information on access management.	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
55.	RIR021 - The entities/providers must guarantee and establish mechanisms to retrieve the information assets in the event of an early termination/expiration and/or indefinite interruption of the services and/or relocation, observing the security conditions of the information and the continued operations.	Google recognizes that regulated entities need to be able to exit our Services (including to transfer services to another service provider) 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 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 and storage options on our Compute Engine Documentation page.	Transition Term Data Export (Cloud Data Processing Addendum)
56.	RIR022 - The resources and information used in the ITS must be inventoried with the respective identification of the owner and stating the parameters for a safe disposal and the validation parameters in the lifecycle of the data.	Google provides tools to help you manage your assets on our services. For example: • Cloud Asset Inventory allows you to view, monitor, and analyze all your GCP and Anthos assets across projects and services. Not only can you export a snapshot of your entire inventory at any point of time, you can also get real-time notifications on asset config changes. • Cloud Data Loss Prevention helps classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance.	N/A
57.	RIR023 - The entities/providers must establish a lifecycle for the data recording the activities, as established in requirement RIR003, in compliance with the legal requirements and security provisions for their storage, inalterability during the legal term of preservation, and the accessibility for those responsible of the control in order to support forensic investigations in the event of security incidents and detection of security breaches.	Refer to Row 28 for information about traceability. In addition, Cloud Audit Logs are encrypted at rest by default and reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. The service is also coupled with Google Cloud's Access Transparency service, which surfaces near real-time logs of GCP administrator access to your systems and data.	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
58.	RIR024 - The entities/providers must establish an encryption policy for data at rest, data in transit or data in both conditions, including the assignment of responsibility for the controls defined at each status of data.	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. Encryption key management We also offer a continuum of encryption key management options to meet your needs. Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation.	Data Security; Security Measures (Cloud Data Processing Addendum)
59.	RIR025 - The entities/providers must guarantee a logical separation of the data processing, storage, transmission, and retrieval environments of the entity with respect to the provider, other entities and third parties. Furthermore, they must guarantee that the devices/equipment and software components used or having access to the entity's environment are limited to those necessary and validated as stated in requirement RIR011.	Logical separation To keep data private and secure, Google logically isolates each customer's data from that of other customers. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information. In addition, refer to our What is Zero Trust Identity Security? blog post for more information about our zero trust system known as BeyondCorp, to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our What is Zero Trust Identity Security? blog post.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
60.	**7.7.5. Monitoring and Control.**		
61.	RMC003 - The entities/providers must follow-up the security setting changes in the ITS and verify the updating levels of: operating systems, databases, communication links, malware prevention and detection tools, network security equipment, traffic controllers, and any other security tool. They must include, for example:		
62.	a) Follow-up of privilege and access rights.	There are a number of ways to perform effective ongoing configuration management using the services: • Cloud Identity and Access Management helps to prevent 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. In addition, 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 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. Refer to Row 3 for more information about Google's security practices.	N/A
63.	b) Information back-up, protection, and retrieval processes.	Refer to row 62 for more information.	N/A
64.	c) Availability of devices/equipment.	Refer to row 62 for more information.	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
65.	d) Alarms, warnings and problems detected by the event registration systems.	Refer to row 62 for more information.	N/A
66.	RMC004 - The entities/providers must provide for transactional monitoring mechanisms in the ITS that operate based on the features of the customer's transactional profile and pattern in any of the following action models:		
67.	a) Preventive. By detecting and triggering actions to communicate with the client through alternative channels before confirming operations.	This is a customer consideration.	N/A
68.	b) Reactive. By detecting and triggering actions to communicate with the client after the confirmation of suspicious operations.	This is a customer consideration.	N/A
69.	c) Assumed. By detecting and assuming the return of the relevant amounts if the customer files a claim denying a transaction.	This is a customer consideration.	N/A
70.	RMC006 - Based on the records collected by the ITS resources associated to the scenario, the entities/providers must classify and determine the security events, and define the limits and thresholds of commitment, and the levels of normal/unexpected behavior, and establish the actions to be taken according to each classification and limit determined.	This is a customer consideration.	N/A
71.	RMC014 - The entities/providers must determine, document and set the relevant processes for the resources, devices/equipment, and software components to monitor the ITS activities.	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. • 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
72.	RMC015 - The entities/providers must formally establish and periodically run tests of and analyze the vulnerabilities of the ITS-related resources in all its critical processes.	Vulnerability management 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	Customer Penetration Testing

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Penetration tests You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	
73.	**7.7.6. Incident Management.**		
74.	RGI001 - Based on the risk analysis of the IT assets related to the scenario, the entities/providers must conduct at least annually an analysis of the incidents occurred and create a report useful to establish protection measures, contents of the training and awareness program, modifications of the event registration and control, and a redefinition of the warnings, limits and thresholds.	Following the successful remediation and resolution of a data incident, the Google incident response team evaluates the lessons learned from the incident. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. Refer to our Data incident response whitepaper for more information.	Data Incidents (Cloud Data Processing Addendum)
75.	RGI002 - The identification of incidents must be based, at least, on early warnings, statistics about type/frequency/pattern of incidents, and IT security recommendations.	Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to our Data incident response whitepaper for more information.	Data Incidents (Cloud Data Processing Addendum)
76.	RGI003 - The management of security incidents may be outsourced, but it must be coordinated with personnel of the financial entity.	This is a customer consideration.	N/A
77.	RGI005 - The incidents detected must be handled as usual and escalated through a formally defined process.	Information on Google's data incident response process is available in our Data incident response whitepaper	N/A
78.	**7.7.7. Minimum Requirements Table for Continued Operations**		
79.	RCO001 - The necessary resources for the creation, maintenance, update, and testing must be available for a plan for the continued processing of data. Such plan must be practicable and functional based on the requirements agreed in the ITS inherent in the entity and governed by the BCRA.	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

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide.	
80.	RCO002 - The entities/providers must define, agree, document, and implement the methods to determine the impact of an event interrupting the organization activities of the entity, the provider or outsourced third parties, which methods shall contemplate the following, for instance:		
81.	i) Identification of critical resources, including operational and control users.	Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Our 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. More information is available in our Infrastructure Design for Availability and Resilience whitepaper. In addition: • Refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes. • You can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	Business Continuity and Disaster Recovery
82.	ii) Identification of all agencies, including processes, applications, peers, and outsourced third parties.	Refer to row 81 for more information.	N/A
83.	iii) Detection of threats to the critical resources.	Refer to row 81 for more information.	N/A
84.	iv) Determination of the impact of scheduled or unscheduled interruptions and their variation through time.	Refer to row 81 for more information.	N/A
85.	v) Setting of a maximum tolerable interruption period.	Refer to row 81 for more information.	N/A
86.	vi) Setting of partial and total retrieval periods.	Refer to row 81 for more information.	N/A

Argentina BCRA - Comunicación A 6375
Circular "A" 6375
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
87.	vii) Setting of the maximum tolerable interruption time for the retrieval of critical resources.	Refer to row 81 for more information.	N/A
88.	viii) Calculation of the resources necessary for the operations and alternative locations to continue and for their eventual restoration.	Refer to row 81 for more information.	N/A
89.	In addition, the primary responsible parties for the processes and critical resources must have active participation, ensuring the full coverage of the ITS associates.	Refer to row 81 for more information.	N/A
90.	RCO003 - The plan for the continued processing of data must consider, among other things, including the following contents:		
91.	a) Manual, logistical, and automated emergency proceedings, according to each process/resource identified and action determined.	Refer to rows 79 and 81 for more information.	N/A
92.	b) Place/site, transfer, and transportation of responsible parties, suppliers, and emergency services and physical and logical resources.	Refer to rows 79 and 81 for more information.	N/A
93.	c) Retrieval/restoration proceedings of the committed resources.	Refer to rows 79 and 81 for more information.	N/A
94.	RCO004 - The plan for the continued processing of data must be tested periodically, at least on an annual basis. The tests must be consistent and coherent with the criteria of requirement RCO002. Tests must also guarantee that all parties responsible for and participating in the continuation and retrieval processes are regularly, permanently, and formally informed.	Google will test our business continuity plan at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. Google will ensure that Google personnel who are relevant to the maintenance and implementation of our business continuity plan are appropriately trained and aware of their roles and responsibilities.	Business Continuity and Disaster Recovery