Financial Superintendence of Colombia - Rules regarding the use of cloud computing services

Google Cloud Mapping

This document is designed to help entities supervised by the Financial Superintendence of Colombia ("**supervised entity**") to consider Financial Superintendence of Colombia: Part I, General Instructions applicable to supervised entities: Chapter VI: Rules regarding the use of cloud computing services ("**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: Sections 3-7 of Chapter VI: Rules regarding the use of cloud computing services.. 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.	**3. GENERAL OBLIGATIONS OF THE ENTITIES**		
2.	The entities that support the operation of their mission processes or accounting and financial management on cloud computing services must:		
3.	3.1 Contemplate within their Operational Risk Management System (SARO) the effective management of the risks derived from the use of cloud computing services, considering, among other factors, the type of cloud acquired, the processing sites, the services hired, the type of information to be processed, the security controls for the protection of data in virtualized environments and the protection of the entity's applications.	Risk management 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 Public cloud GCP is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy GCP as part of a hybrid or multi-cloud deployment. Services The GCP services are described on our services summary page. Processing sites Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. Type of information 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.	N/A Definitions

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Security Refer to Row 8 for more information on Google's security practices.	
4.	3.2 Establish the criteria for selecting the cloud computing 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 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 audited financial statements on Alphabet's Investor Relations page.	N/A
5.	3.3 Asses the advisability of implementing the instructions of this Chapter in their foreign affiliates and subsidiaries, if any.	This is a customer consideration.	N/A
6.	3.4 Verify that the cloud service provider has and keeps up-to-date, at least, the ISO 27001 certification, and others related to compliance with standards or good practices, such as ISO 27017 and 27018. The provider can be certified with standards or best practices that replace, substitute or modify previous standards and must have service organization control reports (SOC1.SOC2 , SOC3)	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	Certifications and Audit Reports

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
7.	3.5 Verify that the provider offers an availability of at least 99.95% in the cloud services provided	Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.	Services
8.	3.6 Manage the risks of APIs or Web Services provided by the cloud service provider.	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. 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; Google's Security Measures (Cloud Data Processing Addendum)

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

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	
9.	3.7 Verify that the jurisdictions where the information will be processed have standards equivalent to or higher than those applicable in Colombia, in relation to the protection of personal data and penalties for acts in breach of confidentiality, integrity and availability of data and computer system.	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.	Data Transfers (Cloud Data Processing Addendum)

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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. 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 Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
10.	3.8 Establish mechanisms that allow the information processed in the cloud to be backed up, information which must be available to the entity when required.	Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	N/A
11.	3.9 Guarantee the independence of their information and backup copies of the information of other entities processed in the cloud. Independence can be given at a logical or physical level.	Refer to Row 10.	N/A
12.	3.10 Keep information that is classified as confidential in transit or at rest encrypted, using internationally recognized standards and algorithms that provide at least the security offered by AES , RSA or 3DES.	Encryption is central to Google's comprehensive security strategy. We provide certain encryption by default, with no additional action required from you. 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. 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	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
13.	3.11 Control the administration of users and privileges for access to the services offered, as well as to the platforms, applications and databases that run in the cloud, depending on the service model acquired.	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.	N/A
14.	3.12 Monitor the services hired to detect unwanted operations or changes and/or take preventive or corrective actions when required.	Our Risk and Compliance as Code (RCaC) Solution stack enables compliance and security control automation through a combination of Google Cloud Products, Blueprints, Partner Integrations, workshops and services to simplify and accelerate time to value. Through the RCaC solution, customers can introduce automation via IaC (Infrastructure as Code) and PaC (Policy as Code) in the form of blueprints. This lays the foundation of preventative controls. The next level of maturity is detection as code which involves monitoring for (security and compliance) drifts and applying remediations when an out-of-compliance infrastructure is identified. This forms a continuous monitoring loop that helps prevent misconfigurations.	N/A

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
15.	3.13 Establish procedures to verify compliance with the agreements and service levels established with the cloud service provider and its subcontractors or partners, when they are in charge of providing the service.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. 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. • **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). Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights).	Services Ongoing Performance Monitoring Google Subcontractors
16.	3.14 Have end-to-end encrypted communication channels with the cloud service provider that use different routes, whenever possible.	Google provides customers with tools that facilitate ubiquitous data encryption which delivers unified control over data at-rest, in-use, and in-transit, all with keys that are under your control.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
17.	3.15 Contemplate within the criteria for selecting the firms that will be in charge of the infernal or external audit of the entity, the technical skills necessary to assess cloud services	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
18.	3.16 Establish the necessary measures to guarantee that, in the event of takeover, the SFC, Fogafin, Fogacoop, or any person designated by any of the foregoing, can access the information and the administration of the information systems that run in the cloud	Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.	Support through Resolution

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
19.	**4. SERVICES AGREEMENTS OR CONTRACTS**		
20.	The agreements or contracts signed by the entities for the provision of cloud computing services must include at least the following elements.		
21.	4.1 The conditions regarding capacity, availability, recovery times, existence of continuity plans, troubleshooting and business hours of the service provider, which must consider service levels so as to comply, at least, with the instructions indicated in section 3 of this Chapter.	Capacity and availability Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. In addition, Google provides tools to help you manage and scale your networks. Refer to our Google Cloud Networking Products page for more information. For example: • Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications. • Dedicated Interconnect is a high-performance option providing direct physical connections between your on-premises network and Google's network. Recovery times Refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired recovery time objective and recovery point objective for your applications. Troubleshooting The support services are described on our Technical Support Services Guidelines page. This includes hours of operation, response times and languages supported. Business continuity plans	Services N/A Technical Support

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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
22.	4.2 The information security and cybersecurity conditions of cloud services and the conditions established to protect the privacy and confidentiality of customer data, which must consider service levels so as to comply, at least, with the instructions indicated in section 3 of this Chapter on the information processed in the cloud.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 8 for more information on Google's security practices.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)
23.	4.3 The ownership of the information that is processed in cloud computing services, making it clear that the data are owned by the supervised entity and cannot be used for any purpose other than as established in the agreement.	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. 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.	Intellectual Property Protection of Customer Data
24.	4.4 The conditions and limitations under which part of the service can be outsourced or changes be made to the agreements established with its subcontractors or partners.	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 will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
25.	4.5 The grounds for termination of the agreement by the entity, including, breach of the agreements or service levels or any change in the conditions generating a negative impact on the service acquired.	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Term and Termination Services

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
26.	4.6 The delivery to the supervised entity of reports and certifications proving the quality, performance and effectiveness in the management of the services acquired, as well as the validity of the certifications set forth in section 3.4 of this Chapter.	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 Reports
27.	4.7 The obligation of the service provider to inform, whenever possible, the supervised entity about any event or situation that could significantly affect the provision of the service and, therefore, the compliance by the supervised entity with its obligations to the financial consumers, the SFC and other entities.	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
28.	4.8 The secure deletion of existing data on the storage media when the agreement ends, when requested by the entity or when the cloud service provider removes and/or replaces said media.	Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. 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 by Customer (Cloud Data Processing Addendum) Deletion on Termination (Cloud Data Processing Addendum)
29.	4.9 The timely and effective correction of detected computer 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	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

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.	(Security Measures) (Cloud Data Processing Addendum)
30.	4.10 The use of multi-factor authentication techniques for access to the administration consoles by the supervised entity	Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Refer to our Multi-Factor Authentication page for more information.	N/A
31.	**5. BUSINESS CONTINUITY MANAGEMENT**		
32.	The supervised entities must consider cloud operation within the business continuity plan and carry out the necessary tests to confirm the effectiveness of the contingent procedures.	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
33.	Likewise, they must have a migration strategy to another platform in place, in case the agreement is terminated by either party, due to the disruption or impairment in the provision of the service by the cloud service provider or for any other reason considered as reasonable by the supervised entity.	We recognize that, whatever the level of technical resilience that can be achieved on GCP, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: ● Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. ● Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. ● Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
34.	**6. TRANSFER OF INFORMATION TO THE SFC**		
35.	Within 15 days prior to the start of the processing of information in the cloud, in relation to mission processes or accounting and financial management, entities must submit the following information to the SFC :		
36.	6.1 The Name of the provider that will deliver cloud services and the subcontractors or partners that will deliver services related to the subject matter of the agreement.	Name of provider Refer to your Google Cloud Financial Services Contract. Subcontractors To enable regulated entities to retain oversight of any subcontracting and provide choices about the services supervised 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.	N/A Google Subcontractors
37.	6.2 The list of the processes to be managed in the cloud, including applications, type of data, products and associated services.	The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
38.	6.3 The physical location or region where the data will be processed and stored.	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.	Data Transfers (Cloud Data Processing Addendum)
39.	6.4 The certifications granted to the service provider and/or processing site.	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
40.	6.5 The list of audits that the hired service provider undergoes.	Refer to Row 39.	N/A
41.	6.6 Information on established service levels.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
42.	6.7 The diagram with the technological platform that will support the services acquired.	Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.	N/A
43.	**7. DOCUMENTATION**		
44.	Entities must keep up-to-date and permanently available to the SFC, through the verifiable means established for such purpose, the information listed below:		
45.	7.1 Complete documentation of the processes and procedures running in the cloud.	You decide which services to use, how to use them and for what purpose. Therefore, you decide which of your processes and procedures run in the cloud. 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. • **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.	N/A
46.	7.2 Documentation of applications that run in the cloud.	Refer to Row 45.	N/A
47.	7.3 The documentation on the data flows of the mission processes or accounting and financial management that feed or consume the applications provided by the cloud service provider, when applicable.	Refer to Row 45.	N/A

Financial Superintendence of Columbia - Rules regarding the use of cloud computing Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
48.	7.4 The network diagrams that allow the platform that supports the service acquired to be identified.	Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.	N/A
49.	7.5 The procedures to verify compliance with the agreements and service levels established with the cloud service provider.	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. • **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
50.	7.6 The general audit reports, vulnerability tests and current status of the services acquired.	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. Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. The **Status Dashboard** provides status information on the Services.	Certifications and Audit Reports Customer Penetration Testing Ongoing Performance Monitoring