CMF - Chapter 20-7

Google Workspace Mapping

This document is designed to help banking institutions supervised by the Comisión Para El Mercado Financiero (“**regulated entity**”) to consider Chapter 20-7 Outsourcing of Services (the “**framework**”) in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Chapter 20-7, III to V, and Annexes 1 and 2. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**CHAPTER 20-7 OUTSOURCING OF SERVICES**		
2.	**III. OUTSOURCING OF SERVICES CONDITIONS**		
3.	The entity that decides to outsource any activity, in addition to considering the aspects indicated in Annex No. 1 for the purpose of contracting each particular service, must comply with the following conditions:	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we’ve provided information for each of the areas you need to consider in the rows that follow. For information on Annex No. 1, refer to Rows 72 to 87.	N/A
4.	**1. General conditions.**		
5.	a) The Board of Directors must decide on the risk tolerance it is willing to assume in the case of outsourcing services.	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
6.	b) Maintain a policy duly approved by the Board of Directors, which regulates the activities associated with outsourcing. This policy must at least address the elements indicated in No. 2 below.	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
7.	c) Verify that the supplier has mechanisms in place to prevent actions carried out by other clients from negatively affecting the service outsourced by the entity.	To keep data private and secure, Google logically isolates each customer's data from that of other customers. For more information on Google’s security practices, refer to Row 52.	N/A
8.	d) Establish formal procedures for supplier selection, contracting and 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: ● The Status Dashboard provides status information on the Services. ● Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.	Ongoing Performance Monitoring

CMF - Chapter 20-7

GoogleWorkspace 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 user content. 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).	
9.	e) Ensure that the supplier and the personnel in charge of the contracted services have adequate knowledge and experience. Likewise, it must also oversee due compliance with regulatory and legal aspects that may affect the provision of contracted services (e.g. labor laws).	Google knowledge and experience • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about Google Cloud's leadership team is available on our Media Resources page. • Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. Your personnel 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
10.	f) Maintain an updated registry of all services contracted with external companies, clearly determining those that, in its opinion, are strategic and high risk, in order to establish permanent control and follow-up procedures according to the levels of criticality assigned to them.	This is a customer consideration.	N/A
11.	g) Establish procedures to ensure timely and full compliance with its commitments to its customers.	This is a customer consideration.	N/A
12.	h) Ensure that there are independent audits of the supplier selection, contracting and follow-up process, with personnel specialized in the different risks audited.	This is a customer consideration.	N/A
13.	i) Ensure that the supplier periodically carries out internal audit reports or independent reviews of its services, in accordance with its structure and the size of its organization and must share relevant findings with the institution in a timely manner.	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)	Certifications and Audit Reports

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
14.	j) Require service providers to ensure that the operational, administrative, and technological procedures of the contracted service are duly documented, updated and permanently available for review by this Commission.	Refer to our Documentation page for technical documentation, including information on service configuration. Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page.	N/A
15.	k) Consider the risks arising from outsourced service chains, which should be reflected in the respective contract in advance, stating that, in the event of outsourcing, the outsourced company must also comply with the conditions agreed between the entity and the initial service provider. Likewise, the responsibilities and obligations to be fulfilled by the subcontracted companies with respect to the service outsourced by the entity must be clearly established in the respective contracts.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. To enable regulated entities to retain oversight of any sub-outsourcing and provide choices about the services they 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 oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors
16.	l) The entity must include in its operational risk reports prepared for the Board of Directors, or whoever is acting in its stead, information regarding the institution's management of outsourcing risks, including changes in the risk profile of suppliers (such as relevant changes in their processes and geographical areas where services are provided) and exposure to those services considered critical.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status Dashboard page.	Significant Developments
17.	m) The data, technological platforms, and applications to be used in the outsourcing of services must be located in specific processing sites and, in the case of offshore processing, in a defined and known jurisdiction. In addition to the jurisdiction, the city where the data centers operate must be known.	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 where your data will be stored is available here.	Data Transfers (Cloud Data Processing Addendum)

CMF - Chapter 20-7

GoogleWorkspace 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. 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 Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
18.	**3. Business continuity.**		
19.	The entity must verify that its critical service providers have appropriate plans to ensure the continuity of the contracted services. Likewise, the entity must verify that its critical service providers ensure that the services subcontracted by them have appropriate business continuity plans. These plans must be tested at least once a year, including, when appropriate, the disaster scenario of its different processing sites, and the entity must take cognizance of such activity and verify the results obtained. In addition, the entity must also have plans, also tested, to ensure operational continuity in the contingency of not having such external service.	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. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired resilience for your applications.	Business Continuity and Disaster Recovery
20.	The entity must have exit plans in the event of non-compliance by such suppliers, which consider the early termination of the contractual relationship and allow the operation to be resumed, either on its own or through another supplier.	We recognize that, whatever the level of technical resilience that can be achieved on Google Workspace, 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.	Data Export (Cloud Data Processing Addendum)

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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 Google Workspace 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.	
21.	The institution must ensure that the supplier has a formal and systematic process for managing incidents that could interrupt or affect the provision of products, services or activities.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status 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 whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
22.	The processing sites and technological infrastructure that support the outsourced services must consider the requirements indicated in Title II of Chapter 20-9 of this Compilation.	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.	Certifications and Audit Reports
23.	**4. Security of its own and its customers' information, where applicable.**		

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24.	The entity must ensure that the service provider maintains an information security program that allows it to ensure the confidentiality, integrity, traceability and availability of its information assets and those of its customers. These conditions must be consistent with the policies and standards adopted by the entity and be incorporated in the service contract.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and integrity of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption.	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **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. (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	

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
25.	The entity must control and monitor the information security infrastructure provided by the supplier, in order to protect the information assets present in the outsourced critical services, regardless of the controls provided by the supplier. Likewise, it must control and monitor the management of identities and access control to the information related to such critical services.	Refer to Row 24 for information on Google's security practices, including regarding the security measures that you can choose to implement and operate when you use the Services. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. 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). 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.	N/A
26.	Communications connections between the procuring entity and the service provider must be encrypted to ensure *end-to-end data* confidentiality and integrity.	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.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	The entity must ensure that the provider has effective control and protection measures against external attacks aimed at making the contracted services unavailable, such as, for example, denial of service attacks. Additionally, for outsourced critical services, the entity must control the periodic performance by the provider of vulnerability assessments of its technological infrastructure and penetration tests.	Incident management Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. Penetration testing Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Data Incidents (Cloud Data Processing Addendum)
28.	Once processed, the information must be stored and transported in encrypted form, and the decryption keys must be kept in the entity's possession. The procedures for exchanging keys between the service provider and the institution must also be defined, in addition to establishing the roles and responsibilities of the persons involved in security management.	The security of your data is of paramount importance to Google. We take the following proactive steps to assist you: • **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google.	N/A
29.	In the case of processing of physical documentation, the entity must have control procedures to ensure due compliance with the conditions set forth in this Title. In addition to the above, procedures must be established to ensure the proper transfer of information to the entity by the supplier, and that in no case the supplier keeps information in its possession after the end of the contractual relationship.	Physical documentation Given the nature of the services, Google does not process physical documentation. Deletion on termination On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Deletion on Termination (Cloud Data Processing Addendum)
30.	**5. Country risk.**		
31.	Services may only be outsourced to jurisdictions with an investment grade country risk rating. Notwithstanding the foregoing, the Board of Directors or the body acting in its stead may waive this requirement, to the extent that the country in which the services are outsourced has adequate personal data protection and security laws, and shall leave a record of the analysis made to that effect. The foregoing, without prejudice to the	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 where your data will be stored is available here.	Data Center Location; Data Transfers (Cloud Data Processing Addendum)

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	provisions of number 2 letter i) of Title III and number 1 letter b) of Title IV of this Chapter.	Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data - including a choice to store your data in Europe. 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 Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
32.	**6. Management responsibility.**		
33.	The responsibility for the overall management of risks and control functions shall be maintained by the entity in the country. The foregoing is without prejudice that in some international entities there may be, for purposes of a consolidated management of their parent companies, matrix coordination between personnel established abroad and local personnel.	This is a customer consideration.	N/A
34.	Furthermore, in compliance with the provisions of Chapter 20-8 of this Compilation, the institution must communicate to this Commission, in the terms defined in said Chapter, the operational incidents that affect an outsourced service in the country or abroad.	Refer to Row 21 for more information on how Google reports significant developments and data incidents.	N/A
35.	**7. Access to information by the supervisor.**		
36.	The procuring entity must ensure that this Commission has permanent access, either through visits to the service providers' facilities or remotely, to all records, data and information that are processed, maintained and generated through an external provider, whether established in the country or abroad.	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 and supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Regulator Information, Audit and Access Customer Information, Audit and Access
37.	In the case of a service provider established abroad, special attention must be paid to the legal restrictions of the host country that may prevent this Commission from visiting the provider or accessing the information and data mentioned in the preceding paragraph. Likewise, as part of the risk management, the entity must incorporate within the analysis those aspects related to the legal risks to which the information subject to banking secrecy or reserve established in the General Banking Law is exposed.	Refer to Row 36 for more information on the audit, access and information rights Google grants to supervisory authorities. These rights apply regardless of the service location. In addition, regulated entities may access their data on the services at any time and may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Customer Information, Audit and Access Regulator Information, Audit and Access

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
38.	**IV. FACTORS TO CONSIDER IN THE OUTSOURCE OF DATA PROCESSING SERVICES.**		
39.	The contracting of external data processing services must be supported by the background information detailed in Annex No. 2 of this Chapter, in addition to considering the factors indicated below.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided information for each of the areas you need to consider in the rows that follow. For information on Annex No. 2 refer to Rows 91 to 116.	N/A
40.	Additionally, in the evaluation carried out by this Commission during its auditing activities, a distinction will be made according to the type of services in question.	This is a customer consideration. Google Workspace is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy Google Workspace as part of a hybrid or multi-cloud deployment.	N/A
41.	**1. Geographic location of supplier**	Information about where your data will be stored is available here.	N/A
42.	**a) Services performed in the country**		
43.	When the data processing service, in whole or in part, is provided by a company located in the country, the institution must verify that the technological infrastructure and systems to be used for data communication, storage and processing offer sufficient security to permanently safeguard business continuity, confidentiality, integrity, accuracy and quality of the information. Likewise, it must verify that the conditions of the service guarantee the timely obtaining of any record, data or information it may need, whether for its own purposes or to comply with the requirements of the competent authorities, as is the case of the information that may be requested by this Commission at any time.	Refer to Row 24 for information on Google's security practices. The same robust security measures apply to all Google facilities, regardless of country / region. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access
44.	As for the contingency Data Processing Center, it must meet the conditions of location and distance from the main Data Processing Center, to ensure operational continuity.	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. For more information, refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper.	N/A
45.	**b) Services performed abroad**		
46.	In the event that the entity outsources data processing services outside the country, it must have at all times the background of the contracted company. In particular, it must maintain the background information that supports the financial soundness of the service provider and that it maintains certifications of quality, security, and appropriate control systems.	Background Refer to Row 9 for more information on Google's background and credentials. Financial soundness You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page. Audit reports	Certifications and Audit Reports

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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) • SOC 1 • SOC 2 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
47.	In addition, the entity must have the background of the project, the service contract and, in the case of subcontracts with third parties, these must also be included.	Background of the project 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. Subcontracts 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 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. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
48.	In order to safeguard the proper functioning of the financial market with all its participants, including customers, institutions that carry out activities considered significant or strategic abroad must keep at the disposal of this Commission the information contained in Annex No. 2 of this Chapter and comply with the following conditions for the outsourcing of services:		
49.	i) There must be a contingency Data Processing Center located in Chile and demonstrate a recovery time compatible with the criticality of the outsourced service. Likewise, recovery times must be evaluated by the entity at least once a year, both for transactional and *batch* processes.	Information about where your data will be stored is available here. For more information on how you can achieve desired recovery times, refer to Row 51.	N/A
50.	In the case of banks that maintain adequate operational risk management in the last evaluation carried out by this Commission, rated in accordance with the provisions of Chapter 1-13 of this Compilation, the Board of Directors or the body acting in its stead may waive this requirement, when it is assured, by means of an annual report, that the entity complies, among other aspects, with the adoption of the following preventive measures:		
51.	a) The recovery time objective (RTO) must be approved by the Board of Directors based on a business impact analysis (BIA) and risk analysis (RIA) that is consistent with the criticality of the outsourced service(s). This must be evaluated and tested at least annually.	Information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired RTO and RPO for your applications.	Business Continuity and Disaster Recovery
52.	b) That the data processing *sites* comply with an operating availability time equal to or greater than the provisions of Chapter 20-9 of this Compilation.	Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.	N/A
53.	c) That the sites *are* in different locations that mitigate both geographic and political risks.	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. For more information, refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper.	N/A
54.	d) That in terms of information security, outsourced services are provided in an environment consistent with the policies and standards adopted by the entity.	For more information on Google's security practices, refer to Row 24.	N/A
55.	The aforementioned report must be prepared by an independent company of recognized prestige and experience in the evaluation of this type of services.	This is a customer consideration.	N/A
56.	*Special considerations*		
57.	In the case of banking entities that maintain outsourced services abroad, under the conditions indicated in this paragraph, and that as a result of a new evaluation are rated in the operational risk area in a category of "Unsatisfactory Compliance" or lower, they	This is a customer consideration.	N/A

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	must inform this Commission about the additional specific measures adopted to ensure the adequate operation of the services.		
58.	For those banking entities that do not have a management qualification in the area of operational risk, and that outsource services abroad, all the preventive measures mentioned above will be applicable to them, with the exception of the qualification in this area.	This is a customer consideration.	N/A
59.	ii) The institution must control and monitor the outsourced service abroad, especially in aspects related to information security, business continuity and operating conditions of the processing center. These activities must be duly substantiated in accordance with the risk management performed for the specific supplier. The above, regardless of the control and monitoring activities carried out by the service provider.	Control You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities regardless of the service location. 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: • The Status Dashboard provides status information on the Services. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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).	Instructions Ongoing Performance Monitoring
60.	**V. ENHANCED DUE DILIGENCE FOR CLOUD SERVICES.**		
61.	Cloud computing encompasses the evolution of several areas of information technology, such as telecommunications networks and microprocessors, with virtualization or abstraction of *hardware* being one of the most relevant. Due to the variety of services that can be accessed through the cloud, such as infrastructure,	Google Workspace is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy Google Workspace as part of a hybrid or multi-cloud deployment.	N/A

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	platform or even *software,* there is a change in the dynamics of the risks associated with the current technological models of banking.	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.	
62.	For the purpose of contracting any type of service through the so-called cloud modality, the entity's Board of Directors must make an annual statement on the risk tolerance it is willing to assume in this type of outsourcing. This statement shall consider an analysis of the data to be stored or processed under this modality and its location.	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
63.	Without prejudice to due compliance with the various requirements contained in this Chapter 20-7, financial institutions may outsource their non- critical services to the public or private cloud without additional considerations to those already mentioned in the preceding headings.	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it.	N/A
64.	In the event that the entity evaluates the contracting of a cloud service for an activity considered strategic or critical, this may also be carried out in public or private cloud mode; however, in these cases, the entity must perform an enhanced due diligence of the provider and the service, which at least considers the following:	Refer to Row 65.	N/A
65.	a) The supplier has recognized prestige and experience in the service it provides.	Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about Google Cloud's leadership team is available on our Media Resources page. Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page.	N/A
66.	b) The contracted supplier has independent, internationally recognized certifications in terms of information security management, business continuity and quality of services that reflect current best practices.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a	Certifications and Audit Reports

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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) • SOC 1 • SOC 2 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
67.	c) Service outsourcing contracts are entered into directly between the contracting institution and the suppliers in order to minimize the risks that could arise from the role of intermediary in this type of service.	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A
68.	d) The entity has legal reports regarding privacy and access to information regulations in jurisdictions where the service is being performed and has evaluated the resolution of legal contingencies in the jurisdictions in which it operates.	For more information on data locations, refer to Row 31.	N/A
69.	e) The entity has ensured that the service provider prepares audit reports associated with the services rendered and that these reports are available for consultation at any time by the contracting entity and this Commission, in the relevant matters.	Refer to Row 66 on audit reports.	N/A
70.	f) Verify that the provider has adequate security mechanisms, both physical and logical, that allow isolating the components of the cloud infrastructure that the entity shares with other clients of the provider, in order to prevent information leaks or events that may affect the confidentiality and integrity of the entity's data.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	N/A
71.	g) Identify data that, due to their nature and sensitivity, must have strong encryption mechanisms.	This is a customer consideration. Refer to Row 28 for more information on the encryption tools available.	N/A
72.	**ANNEX N° 1**		
73.	**MINIMUM ASPECTS TO BE CONSIDERED FOR THE OUTSOURCING OF SERVICES.**		
74.	Before deciding to outsource an activity, an assessment must be made that considers all the agents involved regarding the risks that this decision involves for the institution, as well as the amount of risk involved due to the amounts paid to the external company, the volume of transactions to be processed, the criticality of the service contracted, the concentration of services with the same provider, the concentration of the financial sector in a specific provider, among others.	Risk assessment 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.	N/A

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Concentration risk Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. 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 how Google's approach to open source can help you address vendor lock-in and concentration risk.	
75.	This evaluation must consider the opinion of the area in charge of operational risk management of the audited entity, which must be duly supported.	This is a customer consideration.	N/A
76.	2. Selection of the service provider.		
77.	The institution must evaluate the proposals received according to its requirements and carry out *due diligence* to support the information received from potential suppliers.	Google recognizes that you need to perform a risk assessment before deciding to use our services. To assist you, we've provided information for each of the areas you may need to consider in Rows 8 and 9.	N/A
78.	In the event that a service is contracted with a related entity, the economic conditions must comply with principles of transparency and equity, aspects that must be defined in the policy that regulates the outsourcing of services.	This is a customer consideration.	N/A
79.	3. Contract.		
80.	The entity should ensure that the contract clearly defines the rights and obligations of both parties, containing clear and measurable service level agreements, early termination clauses, as well as an appropriate pricing method for the specific contract. In the event that more than one service is acquired for a single price, the details of the charge for each of such services must be included.	Rights and obligations The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. Service Levels The SLAs provide measurable performance standards for the services and are available on our Google Workspace Service Level Agreement page. Termination Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority. Fees	N/A Services Termination for Convenience Payment Terms

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Refer to your Google Cloud Financial Services Contract.	
81.	Business continuity and information security clauses must also be included, especially those referring to the ownership and confidentiality of information, both its own and that of its clients; restrictions on the use of *software*; secure disposal of client data, when applicable; in addition to establishing a permanent authorization that allows both this Commission and the audited entity to examine in situ, or remotely, as available, at any time, all aspects related to the contracted service.	Business Continuity 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. Information security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Confidentiality Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure. Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. Audit rights 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. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Business Continuity and Disaster Recovery Confidentiality Intellectual Property Rights Deletion on Termination (Cloud Data Processing Addendum) Regulator Information, Audit and Access Customer Information, Audit and Access

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
82.	In addition, the institution should consider veto clauses in the selection of third- party subcontractors by the main supplier.	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
83.	Contracts must clearly establish everything related to the suitability and responsibility of the personnel of the company providing the service, as well as all legal and labor aspects applicable to these contracts in the country or abroad.	Customers can operate the services independently without action by Google personnel. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there are no Google personnel dedicated to delivering the services to an individual customer. Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees.	Personnel Security, Appendix 2: Security Measures (Cloud Data Processing Addendum)
84.	Finally, all contracts, subcontracts and their respective annexes must be in Spanish, or translated into Spanish, with the corresponding signatures of the parties.	This is a customer consideration.	N/A
85.	4. Permanent control.		
86.	Of the supplier: The institution should monitor the supplier's performance and possible changes in the institution's requirements during the life of the contract. The monitoring should include at a minimum: knowledge and analysis of the supplier's latest financial statement and aspects such as observation of the external company's general control environment.	Control You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. 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: • The Status Dashboard provides status information on the Services.	Instructions Ongoing Performance Monitoring

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). Financial statements You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page. Audit reports 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 is audited at least once a year for each audited framework.	Certifications and audit reports
87.	Service: The institution must have procedures that allow it to monitor compliance with the clauses stipulated in the contracts. Monitoring should include at least: service level agreements, contractual provisions, management of operational risk associated with the contracted service and possible changes due to the external environment. Additionally, the existence and adequacy of the procedures for transfer to production and incident escalation must be evaluated and tested at least annually, as well as defining and controlling the relevant milestones for each of these services.	Refer to Row 86 for more information on how you can monitor Google's performance of the Services.	N/A
88.	**Annex No 2**		
89.	**ADDITIONAL BACKGROUND FOR OUTSOURCING DATA PROCESSING SERVICES**		
90.	I. General information		

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
91.	1. Governance structure defined between the entity and the supplier, clearly identifying its strategic, tactical, and operational level, both in the project development stage and in the relationship in regime.	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for. It is important for regulated entities to have a clear understanding of the shared responsibility model, and in particular the boundaries of responsibility between your organization and the cloud service provider. The cloud shared-responsibility model assigns responsibility as follows: ● As your cloud service provider, Google is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. ● You are responsible for managing the risks and controls of your environment in the cloud, such securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	N/A
92.	2. Detailed cost structure of current and post-processing data processing (for the same items considered).	Refer to your Google Cloud Financial Services contract. Refer to our Pricing page for more information.	Payment Terms
93.	II. Project information		
94.	1. Detailed scope of the external processing service.	The Google Workspace 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
95.	2. Detailed identification of the business platforms and applications that will be processed externally and those that will remain within the institution.	Refer to Row 96 above.	N/A
96.	3. Supporting documents of the external processing project, which must be in accordance with the project management methodology adopted by the entity.	Refer to our Documentation page for technical documentation, including information on service configuration.	N/A
97.	4. Detail of the items to be considered in the respective tariff agreement.	This is a customer consideration.	N/A
98.	5. Risk analysis and evaluation report carried out by an independent entity. This report must include the project's risk matrix, which must include at least the identification of the outsourced processes, the identification of the sources and risk factors that affect them, the inherent risk, the impact and probability of occurrence, and an evaluation of the design and operation of the controls to determine the resulting residual risk.	This is a customer consideration.	N/A
99.	6. Technical and financial evaluation of the project.	This is a customer consideration.	N/A
100.	7. Evaluations carried out for the selection of suppliers.	Google recognizes that you need to perform a risk assessment before deciding to use our services. To assist you, we've provided information for each of the areas you may need to consider in Rows 8 and 9.	N/A

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
101.	8. Details of the transfer methodology used, if applicable (hardware, software, and telecommunications).	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.	N/A
102.	9. Test and simulation certification methodology.	This is a customer consideration.	N/A
	10. Acceptance criteria established for each sub-stage and activities that make up the project.	This is a customer consideration.	N/A
103.	11. Service contract (including all annexes) and in the case of subcontracts with third parties, these must also be included.	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A
104.	12. Information security and business continuity policies of the service provider.	Refer to Row 24 for more information about Google's security practices. Refer to Row 19 for more information on business continuity.	N/A
105.	13. Description, background and detailed technical characteristics of the service provider's production and contingency site and its certifications.	Information about where your data will be stored is available here. Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes. 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. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	N/A
106.	14. Detailed GANTT letter of the outsourcing project.	This is a customer consideration.	N/A
107.	15. Process and tools that allow the entity to control the application of its policies and good practices in the company providing the service.	For more information on how you can control the Services, refer to Row 86.	N/A
108.	16. Process and tools that will allow you to control compliance with the service levels committed to in the contract.	For more information on how you can monitor the Services, refer to Row 86	N/A
109.	17. Organizational structure that will be in charge of hardware, software, and communications maintenance, especially at the beginning of the external process.	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.	N/A

CMF - Chapter 20-7

GoogleWorkspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
110.	18. Policies and procedures to be used for the maintenance of operational and commercial software, both for those of an evolutionary and corrective nature.	Refer to Row 111 above.	N/A
111.	19. Business continuity plan to be adopted by the institution in the event of a contingency that prevents processing by the supplier or its subcontractors.	We recognize that, whatever the level of technical resilience that can be achieved on Google Workspace, 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 Google Workspace 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)
112.	20. Contingency plans foreseen to maintain the operational continuity of the contracting entity in case of communication or information storage failures	Refer to Row 113 above.	N/A