



Banco de España - Circular No. 2/2016

Google Cloud Mapping

This document is designed to help credit institutions supervised by the Banco de España (“regulated entity”) to consider [Banco de España Circular No. 2/2016](#) (“framework”) in the context of Google Cloud Platform (“GCP”) and the Google Cloud Financial Services Contract.

We focus on Rule 43 of Banco de España Circular No. 2/2016 of the framework. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
Rule 43 (Delegation of the provision of services or of the exercise of functions)			
1.	43.1 The delegation of provision of services or the exercise of the functions of credit institutions to a third party shall be governed by the provisions of Article 22 of Royal Decree 84/2015. Additionally, the provisions of this Regulation must be taken into account, in accordance with the scope of application defined in Rule 2 (Norma 2).	We provide commentary to help you understand how you can address these requirements using the Google Cloud services and the Google Cloud Financial Services Contract in the rows that follow.	N/A
2.	43.2 Entities that have delegated the provision of services or the exercise of functions, including delegation within the group itself, must have a delegation policy approved by its board of directors, subject to periodic updates that will be carried out at least every two years.	This is a customer consideration.	N/A
3.	43.3 In the development of this policy in relation to the provision of services or the exercise of essential functions, the entity shall evaluate the potential impact of any risk incurred and specify the management that, according to its materiality, shall apply to these. At least, the following should be considered:		
4.	43.3 a) The risk of non-compliance with the rules that regulate the activity of the entity and the most relevant standards that apply to the service provider.	<p>You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities.</p> <p>Regulated entities can use the following functionality to control the Services:</p> <ul style="list-style-type: none"> • Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources. • gcloud Command Tool: A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer’s operating system. • Google APIs: Application programming interfaces which provide access to GCP. <p>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.</p> <p>For more information on the security standards that Google adheres to, refer to Row 8.</p>	<p>Instructions</p> <p>Representations and Warranties</p>
5.	43.3 b) The risk of concentration derived from the accumulation of services or functions delegated to the same provider or in the same geographical area.	To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud .	Data Export (Cloud Data Processing Addendum)



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> <ul style="list-style-type: none"> • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. 	
6.	43.3 c) The risk inherent to the country in which the service provider is located.	<p>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.</p> <ul style="list-style-type: none"> • Information about the location of Google's facilities and where individual GCP services can be deployed is available here. • Information about the location of Google's subprocessors' facilities is available here. <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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).</p> <p>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 European customers on Google Cloud Whitepaper.</p>	<p>Data Transfers (Cloud Data Processing Addendum)</p> <p>Data Security; Subprocessors (Cloud Data Processing Addendum)</p> <p>Data Location (Service Specific Terms)</p>
7.	43.3 d) The reputational risk derived from the practices followed by the service provider that could generate a negative opinion about the entity in customers, investors, the supervisor or the market in general.	<p>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. Refer to Row 11 for more information on Google's expertise and experience in providing cloud services.</p>	N/A



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
8.	43.3 e) Operational risk, including legal risk, due to failures in the provision of the service by the provider, as a consequence, among other factors, of the inadequacy of the processes, internal systems or assigned personnel.	<p>You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard. Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper</p> <p>In addition, Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none"> • 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 <p>You can review Google's current certifications and audit reports at any time.</p>	<p>N/A</p> <p>Certifications and Audit Reports</p>
9.	43.3 Likewise, the control unit of the area or the receiver of the service responsible for monitoring and controlling any of the functions or services that are delegated must be specified.	<p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <ul style="list-style-type: none"> • The Status Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number 	Ongoing Performance Monitoring



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).</p> <p>For more information on the third-party audit reports that Google provides, refer to Row 8.</p>	
10.	43.4 In relation to the delegation of the provision of services or the performance of essential functions, the board of directors must ensure compliance with the requirements established in its policy regarding the delegation of services or functions through follow-up reports, which will be prepared by the relevant internal department. Internal audit will review the content of these reports, which may vary both in frequency and in depth, depending on the nature or criticality of the services or delegated functions, but which will have to evaluate both the risks and the benefits obtained with the delegation and they should be updated, at least annually.	This is a customer consideration.	N/A
11.	43.5 In the selection of service providers or functions, whether or not they are essential, the entities must assess, among other factors that may be relevant in each case, the quality, experience and stability of the suppliers and the degree to which they comply with the most relevant laws and regulations that apply to them. In particular, the manner in which compliance with the rules on the prevention of money laundering and client protection must be assessed.	<p><u>Quality, Experience and Stability</u></p> <p>Information about Google Cloud's service delivery capability and effectiveness is available on our Choosing Google Cloud page.</p> <p>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.</p> <p>Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page.</p> <p>Information about Google Cloud's leadership team is available on our Media Resources page.</p> <p>You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.</p> <p><u>Compliance with laws and regulations</u></p> <p>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.</p>	<p>N/A</p> <p>Representations and Warranties</p>
12.	43.6 The delegation of the provision of services or of the performance of essential functions can not result in the obstruction of the powers of supervision of the competent authority or in the excessive dependence of the entity on the service provider. For this purpose, the contracts of the Spanish entities that regulate the activity must:	Google recognizes that regulated entities and supervisory authorities must be able to audit our services effectively. Nothing in our contract is intended to impede or inhibit the supervisory authority's ability to supervise our services effectively.	Enabling Customer Compliance
13.	43.6 a) Include a clause that contemplates the direct access and without restrictions of the competent authority to the information of the credit institution in the hands of the	Google grants audit, access and information rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used	Regulator Information, Audit and Access;



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	suppliers, as well as the possibility of verifying, in the premises of these, the suitability of the systems, tools or applications used in the provision of the delegated services or functions.	to provide the Services to conduct an on-site audit. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Customer Information, Audit and Access
14.	43.6 b) Allow the withdrawal and provide for reasonable withdrawal costs for the entity.	<p><u>Ceasing use of service</u></p> <p>If you wish to stop using our services you may do so at any time.</p> <p><u>Termination</u></p> <p>Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority.</p> <p><u>Withdrawal</u></p> <p>Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.</p> <p>Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> <ul style="list-style-type: none"> • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. 	<p>Ceasing Services Use</p> <p>Termination for Convenience</p> <p>Transition Term</p> <p>Data Export (Cloud Data Processing Addendum)</p>
15.	43.6 c) Allow the entity to limit the subcontracting of services by the service provider or extend the principles of its delegation policy to these cases.	<p>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services they use, Google will:</p> <ul style="list-style-type: none"> • 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



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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, and security requirements).	
16.	43.6 d) Include the requirement that the service provider have a contingency plan that allows them to maintain their activity and limit the losses of the entity in case of serious incidents.	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.	Business Continuity and Disaster Recovery
17.	43.6 Additionally, if the supplier is located abroad, a clause must be included that specifies the jurisdiction of the country to which the contract will be subject, so that the entity knows the potential legal risks it may incur in case of conflict.	Refer to your Google Cloud Financial Services Contract.	Governing Law
18.	43.7 Entities shall ensure that their own contingency plans include and adequately contemplate the services or functions that have been delegated, in particular those that are essential, and establish alternatives to the contracted delegation.	Information about how customers can use our Services in their own business contingency planning is available on the Google Cloud Platform Disaster Recovery Planning Guide page and our Strengthening Operational Resilience in Financial Services whitepaper . As part of your contingency planning, you can choose to use Anthos build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments.	N/A
19.	43.8 Depending on the nature or criticality of some functions or services, or their effects on the internal governance regime of the entity, the competent authority may establish limitations to the delegation, for which purpose it will take into consideration, among other aspects, the delegation policy established by the entity, its organizational structure, its internal control environment and the implications of the delegation in relation to the exercise of the supervisory function of the competent authority.	This is a customer consideration.	N/A
20.	43.9 Entities must formally inform the competent authority, at least one month in advance, of their plans to delegate essential functions or services. This communication must be accompanied by the corresponding risk analysis and the mitigating measures that may be appropriate, especially when the delegation involves the use of new technologies.	This is a customer consideration. 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. The security of a cloud service consists of two key elements: <u>(1) Security of Google's infrastructure</u> 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.	N/A Data Security; Security Measures (Cloud Data Processing Addendum)



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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.</p> <p>More information is available at:</p> <ul style="list-style-type: none">• Our infrastructure security page• Our security whitepaper• Our cloud-native security whitepaper• Our infrastructure security design overview page• Our security resources page <p>In addition, you can review Google's SOC 2 report. Refer to Row 8.</p> <p><u>(2) Security of your data and applications in the cloud</u></p> <p>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.</p> <p><u>(a) Security by default</u></p> <p>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:</p> <ul style="list-style-type: none">• Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption.• Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. <p><u>(b) Security products</u></p> <p>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.</p>	



Banco de España - Circular No. 2/2016

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>(c) Security resources</p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none">• Security best practices• Security use cases	