# Banco de España - Circular No. 2/2016

## Google Workspace 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 Workspace 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. | You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities.<br><br>Regulated entities can use the following functionality to control the Services:<br><br>• Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace res<br><br>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.<br><br>For more information on the security standards that Google adheres to, refer to Row 8. | Instructions<br><br>Representations and Warranties |
| 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. | Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page.<br><br>In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services. | Data Export (Data Processing Amendment) |
| 6. | 43.3 c) The risk inherent to the country in which the service provider is located. | 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 (Data Processing Amendment) |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | • Information about the location of Google's facilities is available here.<br>• Information about the location of Google's subprocessors' facilities is available here.<br><br>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:<br><br>• The same robust security measures apply to all Google facilities, regardless of country / region.<br>• Google makes the same commitments about all its subprocessors, regardless of country / region.<br><br>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).<br><br>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Trusting your data with G Suite whitepaper. | Data Security; Subprocessors (Data Processing Amendment)<br><br>Data Location (Service Specific Terms) |
| 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. | 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. | N/A |
| 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. | 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.<br><br>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:<br><br>• ISO/IEC 27001:2013 (Information Security Management Systems)<br>• ISO/IEC 27017:2015 (Cloud Security) | N/A<br><br>Certifications and Audit Reports |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | • ISO/IEC 27018:2014 (Cloud Privacy)<br>• SOC 1<br>• SOC 2<br>• SOC 3<br><br>You can review Google's current certifications and audit reports at any time. | |
| 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. | You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.<br><br>For example:<br><br>• The **Status Dashboard** provides status information on the Services.<br><br>• **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.<br><br>• **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).<br><br>For more information on the third-party audit reports that Google provides, refer to Row 8. | Ongoing Performance Monitoring |
| 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. | Quality, Experience and Stability<br><br>Information about Google Cloud's service delivery capability and effectiveness is available on our Choosing Google Cloud page. | N/A |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | 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.<br><br>Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Cloud Customer page.<br><br>Information about Google Cloud's leadership team is available on our Media Resources page.<br><br>You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.<br><br>Compliance with laws and regulations<br><br>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. | Representations and Warranties |
| 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 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. | 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. 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; Customer Information, Audit and Access |
| 14. | 43.6 b) Allow the withdrawal and provide for reasonable withdrawal costs for the entity. | Ceasing use of service<br><br>If you wish to stop using our services you may do so at any time.<br><br>Termination<br><br>Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority.<br><br>Withdrawal<br><br>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. | Ceasing Services Use<br><br>Termination for Convenience<br><br>Transition Term |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page.<br><br>In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services. | Data Export (Data Processing Amendment) |
| 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. | To enable regulated entities to retain oversight of any subcontracting and provide choices about the services they use, Google will:<br><br>• provide information about our subcontractors;<br>• provide advance notice of changes to our subcontractors; and<br>• give regulated entities the ability to terminate if they have concerns about a new subcontractor.<br><br>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). | Google Subcontractors |
| 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.<br><br>More information on the reliability of the Services is available on our Google Cloud Help page. | 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 |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| 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.<br><br>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.<br><br>The security of a cloud service consists of two key elements:<br><br>(1) Security of Google's infrastructure<br><br>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.<br><br>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.<br><br>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.<br><br>More information is available at:<br><br>● Our infrastructure security page<br>● Our security whitepaper<br>● Our cloud-native security whitepaper<br>● Our infrastructure security design overview page<br>● Our security resources page<br><br>In addition, you can review Google's SOC 2 report. Refer to Row 8.<br><br>(2) Security of your data and applications in the cloud<br><br>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.<br><br>(a) Security by default<br><br>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:<br><br>● **Encryption at rest.** Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or | N/A<br><br>Data Security; Security Measures (Data Processing Amendment) |

# Banco de España - Circular 2/2016

## Google Workspace Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys.<br><br>• **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google<br><br>(b) Security products<br><br>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.<br><br>(c) Security resources<br><br>Google also publishes guidance on:<br><br>• Security best practices<br>• Security use cases | |