Bank of Italy - Circular No. 285

Google Cloud Mapping

This document is designed to help banks supervised by the Bank of Italy ("**regulated entity**") to consider Circular No. 285 of December 17, 2013 (the "**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: VI. The Outsourcing of the Information System. 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	**VI THE OUTSOURCING OF THE INFORMATION SYSTEM**		
2	**1. Introduction**		
3	The outsourcing of ICT resources and services can assume various forms depending on the architectural model and the strategies of outsourcing adopted by the intermediary: vertical outsourcing (relative to certain operating processes), horizontal outsourcing of transversal services like the management of the hardware infrastructure (facility management), the development and the management of the application park (application management), the network connectivity, the technical help desk and the interventions of repair and maintenance of ICT resources, up to the full outsourcing of the overall information system business. Cloud computing (cloud services) is also relevant, a model that allows widespread, convenient, flexible and on-demand network access to a shared group of IT resources (e.g. networks, servers, memories, applications and services), which are made available quickly, with a minimum of management activity or interaction with the service provider.	The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	N/A
4	Banks that resort to the outsourcing of the information system, both in case of full outsourcing and of outsourcing of critical components of the information system, shall comply with the rules on outsourcing of business functions set out in Chapter 3, Section IV. The rules referred to in par. 2 specify, with particular reference to the ICT resources and services, the information obligations provided for in general by the EBA Guidelines on outsourcing.	For more information on compliance with the EBA requirements refer to our EBA Outsourcing Guidelines mapping.	N/A
5	When using a cloud computing model, banks shall define the data and systems security requirements under the outsourcing agreement and constantly monitor compliance with them; the banks shall also adopt a risk-based approach with reference to the place (country and region/location) where the data are stored and processed and to information security.	Data and systems security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers.	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems) ● ISO/IEC 27017:2015 (Cloud Security) ● ISO/IEC 27018:2014 (Cloud Privacy) ● PCI DSS ● SOC 1 ● SOC 2 ● SOC 3 You can review Google's current certifications and audit reports at any time. (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.	

#	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. More information is available at https://cloud.google.com/security/encryption-in-transit. (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 Monitoring For more information on how you can monitor Google's performance of the service refer to Row 10. Locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available here. • Information about the location of Google's subprocessors' facilities is available here. 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	N/A Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 on Google Cloud Whitepaper.	Data Location (Service Specific Terms)
6	**2. Agreements with suppliers and other requirements**		
7	Without prejudice to the provisions of Chapter 3, Section IV, with reference to the outsourcing of the information system, it should also be noted that:		
8	a. the following aspects shall be clearly defined and formalized in the written agreement between the bank and the suppliers of ICT systems and services:		
9	i. the service provider's risk mitigation measures, which must comply with the bank's risk management framework, with particular regard to ICT and security;	For more information about security and how this is addressed in our contract refer to Row 5.	N/A
10	ii. appropriate measures to ensure accountability and traceability of the operations performed, at least with reference to critical operations and access to personal or sensitive data;	Accountability You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services. For example: ● The **Status Dashboard** provides status information on the Services. ● **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. Traceability Google recognizes that you need visibility into who did what, when, and where for all user activity on our service.	Ongoing Performance Monitoring N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	
11	iii. the obligation for the service provider, once the contractual relationship is terminated and an agreed period of time has elapsed, to eliminate - by making use of appropriate tools and technical solutions, duly documented - any copy or excerpt of personal or sensitive data on its systems or media in connection with services previously outsourced by the Bank, so as to exclude any subsequent access by its staff or third parties;	On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
12	iv. the allocation of tasks and responsibilities relating to the implementation of the Bank's Information Security policy;	The Cloud Data Processing Addendum address the task and responsibilities of the parties for security. For more information about security and how this is addressed in our contract refer to Row 5.	N/A
13	v. the link with the roles and procedures of the intermediary relevant to the ICT risk analysis process (see Section III) and for the data management system (see Section V);	This is a customer consideration. You decide which of our services to use, how to use them and for what purpose. Therefore, you decide the link between our services and your internal process and systems. There are a number of ways to integrate our services with your systems and to perform effective access management. Integration	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		- Cloud Console allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage. - Cloud APIs allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. Access management - Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. - Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. - Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.	
14	b. the notice to the European Central Bank or the Bank of Italy (see Chapter 3, Section IV, paragraph 2), signed by the legal representative of the bank, shall certify the compliance of the transaction with the applicable supervisory regulations and shall include the information indicated below:		
15	i. the results of the risk assessment of the outsourcing agreement conducted by the bank in accordance with Section 12.2 of the EBA Guidelines on outsourcing;	This is a customer consideration.	N/A
16	ii. description of the bank's exit strategies, the bank's outsourcing strategies, the reference model for the information system as modified by the outsourcing and the operating processes of the outsourced services, with particular regard to how the requirements set out in this Chapter are ensured.	This is a customer consideration.	N/A
17	In the report on the controls performed on the functions outsourced to service providers outside the group (see Chapter 3, Section IV, paragraph 2), the bank shall describe, *inter*	This is a customer consideration.	N/A

Bank of Italy - Circular No. 285

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	alia, the information system outsourcing initiatives that have been the subject of prior disclosure as well as the main ICT services provided by third parties that do not qualify as outsourcing.		