Turkey BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

This document is designed to help banks supervised by the Banking Regulation and Supervision Agency ("**regulated entity**") to consider the Regulation on Banks' Information Systems and Electronic Banking Services ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on Article 29 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
1	**Article 29: Regulation on Banks' Information Systems and Electronic Banking Services**		
2	(1) The bank's senior management shall establish an adequate surveillance mechanism that enables it to adequately evaluate and manage the risks to be posed by the services to be procured as outsourced services to the bank and to maintain relations with the outsourced service provider effectively. Within the scope of outsourcing, the following shall be provided:	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.	N/A
3	a) Evaluating all aspects of the risks posed by the outsourced service to be procured,	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
4	b) Exercising due care in the selection of the outsourced service provider,	This is a customer consideration. To assist, we've provided the following relevant information: • Information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. • Information about Google Cloud's leadership team is available on our Media Resources page.	N/A
5	c) Indicating the outsourced service providers and their service areas, contact information and expiry dates of services in writing,	Services The GCP services are described on our services summary page. Expiry date Refer to your Google Cloud Financial Services Contract.	Services Term and Termination
6	ç) Regularly monitoring the accessibility, performance, quality, compliance with the undertaken service levels of the services subject to outsourced services, security breach events within the scope of these services, security controls related to confidentiality,	Performance monitoring You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services.	Ongoing Performance Monitoring

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	integrity and accessibility of the outsourcing service provider, whether its operational and financial situation is suitable to fulfill its obligations and compliance with the terms of the contract,	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. • 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). Security breach events 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. Security controls Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Data Incidents (Cloud Data Processing Addendum) Certifications and Audit Reports

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Financial situation You can review information about Google's financial performance and condition on Alphabet's Investor Relations page. This provides information about our financial strength and sustainability, our areas of investment and growth as well as risk factors.	
7	d) Ensuring the systems and processes within the scope of outsourcing are in compliance with the bank's risk management, security and customer privacy policies,	This is a customer consideration	N/A
8	e) In cases where it is necessary to transfer the bank data to the outsourced service provider within the scope of outsourcing, taking the necessary measures to ensure that the security principles and practices of the outsourced service provider are at least at the level applied by the bank,	The confidentiality and 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. 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.	Data Security; Security Measures (Cloud Data Processing Addendum)

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(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. • **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	
9	f) In case the activities within the scope of outsourcing are carried out within the bank, subjecting the outsourced service provider to the same audits as the bank is envisaged to be subjected to,	Google recognizes that supervisory authorities must be able to audit our services effectively. Google grants audit, access and information rights to supervisory authorities and their appointees.	Regulator Information, Audit and Access
10	g) Arranging the matters related to outsourcing by considering the bank's business continuity plan and taking the necessary precautions,	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.	Business Continuity and Disaster Recovery

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 reliability outcomes.	
11	ğ) Determining an exit strategy suitable for the management of the risks related to the cease or interruption of the outsourcing service out of the planned schedule,	Google recognizes that regulated entities must plan for situations where their providers are unable, for any reason, to provide the services contracted. Google is committed to addressing customers' needs for portability and interoperability. We 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: • 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. In addition, Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	Data Export (Cloud Data Processing Addendum)
12	h) Allowing the transfer of the outsourced service to subcontractors only if the bank permits,	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 subcontracting and provide choices about the services regulated entities use, Google will:	Google Subcontractors

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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.	
13	(2) The terms, scope and any other definitions regarding outsourcing shall be subject to a written contract. The contract includes, as a minimum, the following:		
14	a) Definitions of service levels,	The SLAs are available on our Google Cloud Platform Service Level Agreements page.	Services
15	b) Termination terms of the service,	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period, if Google experiences a change of control, and for Google's insolvency. In addition, regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.	Term and Termination
16	c) Provisions regarding the measures to be taken by the outsourced service provider to prevent disruption of the bank's 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.	Business Continuity and Disaster Recovery
17	ç) Requirements regarding sensitive issues within the security policy of the bank and provisions that will ensure that the outsourced service provider abides by the confidentiality of the information that it learns about the bank and its customers, both during the service and in case of termination of the service	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 8 for more information. Google's commitments to protect customer data in the Cloud Data Processing Addendum remain in effect until the data is deleted.	Duration (Cloud Data Processing Addendum) Confidentiality; Survival

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, Google's confidentiality obligations survive expiry or termination of the contract.	
18	d) Provisions to promptly notify the bank of events such as security breaches or data leaks within the outsourced service provider premises,	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.	Data Incidents (Cloud Data Processing Addendum)
19	e) Provisions regarding the ownership of the products and services subject to the contract and intellectual property rights,	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications.	Intellectual Property
20	f) Provisions that will ensure that the provisions that constitute an obligation for the outsourcing service provider are included as binding articles in the contracts to be executed with subcontractors as well,	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors
21	g) Provisions regarding the management of risks arising from cease or interruption of the outsourcing outside the planned schedule,	Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. 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. Refer to Row 11 on exit strategies for more information.	Transition Term
22	ğ) Provisions that will ensure that bank and customer data are properly returned to the bank and destroyed in case the service procured is terminated,	Deletion 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. Transfer We 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: • 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.	Deletion on Termination (Cloud Data Processing Addendum) Data Export (Cloud Data Processing Addendum)

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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.	
23	h) Provisions that will ensure that the provisions of the legislation to which the bank is subject are also applicable for the outsourced service providers within the framework of the service procured,	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
24	ı) Provisions regarding outsourced service providers providing all kinds of information and documents requested by the BRSA regarding their activities in a timely and accurate manner, and making available for examining and operating the necessary systems and passwords for accessing and making the records legible in all kinds of electronic, magnetic and similar medium.	Google recognizes that regulated entities 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. 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
25	i) Provisions indicating that the bank and its independent auditor are authorized to request all kinds of information and documents from the outsourced service provider regarding the subject from which the outsourced service is procured.	Refer to Row 24.	N/A
26	(3) The Bank cannot procure critical services and outsourced service models carried out within the framework of standard contracts, where it cannot enforce the obligations that are required to be included in the contract indicated in the second paragraph and cannot conduct critical work flows through such outsourced service models.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance
27	(4) The Bank checks whether the providers such as search engines and social media platforms that it wishes to receive advertisement services for the banking services, have taken measures to prevent false advertisements given on behalf of the bank, and cannot receive advertising services from providers that do not take appropriate measures. In the contracts it will execute with providers such as search engines and social media platforms from which it receives advertising services, the bank must include provisions stating that it may obtain the necessary information specific to the event to protect the customer in case of false advertisements. The provisions of this paragraph are also valid for the agreements made with the intermediary firms that the bank has agreed to receive advertising services in this context.	GCP is not an advertising service.	N/A

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
28	(5) The Bank makes the necessary organizational changes to keep the risks arising from outsourcing under control, defines the administrative procedures and appoints a person in charge with sufficient knowledge and experience to conduct relations with the outsourcing service provider in line with the principles defined by its security policy.	Risk management Google provides a number of tools to enable regulated entities to effectively manage risk. There are a number of ways to perform effective access / configuration management using the services: • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. • Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the In addition, 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 here. Here are some examples: • Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. • Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. • Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	N/A

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Knowledge 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.	
29	(6) The types of access rights granted to the outsourced service provider are considered specifically. A risk assessment shall be made for such accesses, which may be physical or logical, and additional controls are established as per the result of the risk assessment. While conducting risk assessment, the type of access needed, the value of the data accessed, the controls conducted by the outsourced service provider, and the effects of this access on the security of bank information shall be taken into consideration.	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies. 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.	Protection of Customer Data Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
30	(7) The Bank is obliged to take the necessary measures to ensure the security of confidential information belonging to itself and its users in scope of the outsourcing. The authority to access the system, access or view data to be granted to outsourced service providers shall be limited to cover the information required by the relevant service. It is the bank's responsibility to ensure that measures are taken by the outsourced service provider to protect the confidential information of the organization and its users.	Refer to Row 8 for information about Google's security practices and Row 29 for information about access control.	N/A

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
31	(8) IS internal control and internal audit activities stipulated within the scope of this Regulation cannot be subject to outsourcing service procurement and are performed by the bank's own personnel.	This is a customer consideration.	N/A
32	(9) The bank's information systems can be subject to outsourcing as a whole or in part, under the following conditions:		
33	a) In terms of banking activities and obligations required by the banking legislation, the bank has the authority of decision-making and the dominant role without any limitation on matters such as management, content design, access, control, auditing, updating, receiving information/reports on the bank's information systems,	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. Regulated entities can use the following functionality to control the Services: • 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.	Instructions
34	b) The bank has knowledge of all administrative details regarding the information systems subject to outsourcing service procurement,	This is a customer consideration. Google provides documentation to explain how customers and their employees can use our services.	N/A
35	c) Establishing an authorization mechanism that will ensure that the bank's access to databases and data, regardless of being critical data or not, is authorized in line with the bank's own permissions, and the bank itself performs internal audit activities such as authorizing all applications used by the bank and reviewing track records,	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. • Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. Refer to Row 29 for more information about how you can manage and monitor Google's access to your data.	N/A

BRSA - Regulation on Banks' Information Systems and Electronic Banking Services

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
36	ç) The ownership of all kinds of information and documents related to accounts, records and transactions formed within the scope of the outsourced service procured, without prejudice to the intellectual property rights regarding the software, belongs to the bank.	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications.	Intellectual Property
37	(10) Utmost care is taken to ensure that the products and services to be procured within the scope of critical information systems and security are produced in Turkey or that the providers have their R&D centers in Turkey, and it is considered as an important criterion in outsourcing service procurement. It is required that such providers and manufacturers have response teams in Turkey. BRSA is authorized to set additional requirements for security products and other IT elements to be used by banks.	You can learn more about Google's presence and long-term commitment in Turkey on our Google in Turkey page.	N/A
38	(11) The bank may use cloud computing services as an outsourced service. Cloud service for primary or secondary systems can be procured with a special cloud service model through hardware and software resources allocated to a single bank. On the other hand, outsourcing through a community cloud service model, in which hardware and software resources allocated to organizations under the supervision of the BRSA are physically shared, but logically, sources were specifically allocated to each bank, is subject to BRSA'a approval. BRSA is authorized to change the organizations that may be included in the community cloud service when it deems necessary.	GCP is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy GCP as part of a hybrid or multi-cloud deployment. To keep data private and secure, Google logically isolates each customer's data from that of other customers. Our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. In addition, our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the role that a well-executed migration to Google Cloud can play in strengthening operational resilience.	N/A