



Korean Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

This document is designed to help financial companies supervised by the Financial Supervisory Service (“**regulated entity**”) to consider the [Regulation on Supervision of Electronic Finance](#) (“**framework**”) in the context of Google Cloud (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Exhibit 2-5 (Key items to be stipulated in the cloud computing service contract). 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.	When a financial company concludes a consignment contract with a cloud computing service provider, the following shall be included. However, only basic items are included when classified as non-critical tasks according to Article 14-2 (1) 1. When classified as a critical task, both basic items and additional items shall be included.		
2	a. Basic items		
3.	Overview of tasks and systems subject to cloud service use	The Google Cloud 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
4.	Matters concerning entrusted business data	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account. The Cloud Data Processing Addendum contains Google’s commitments to protect your data, including regarding security.	Cloud Data Processing Addendum
5.	Matters that need to be notified if there are important changes to the cloud contract and subcontracting	<u>Contractual changes</u> As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties. <u>Subcontracting</u> Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: <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.	Changes to Terms; Amendments Google Subcontractors
6.	Obligation to conduct investigations and access by supervisory authorities or internal and external auditors	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access 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.	Customer Information, Audit and Access; Regulator Information, Audit and Access



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>In addition, 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:</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. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.</p>	Certifications and Audit Reports
7.	Coordination matters such as emergency response training, vulnerability analysis and evaluation, and incident response training	<p><u>Emergency Response Training</u></p> <p>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.</p> <p>Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including:</p> <ul style="list-style-type: none">- destruction of infrastructure required to provide the Services- interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures)- unavailability of key personnel- emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake)- pandemics <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> <p><u>Vulnerability analysis and evaluation</u></p>	Business Continuity and Disaster Recovery



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Refer to our security whitepaper for more information.</p> <p>In addition, you can perform penetration testing of the Services at any time without Google's prior approval.</p> <p><u>Incident response mechanisms</u></p> <p>At Google, we strive to learn from every incident and implement preventative measures to avoid future incidents. The actionable insights from incident analysis enable us to enhance our tools, trainings and processes, Google's overall security and privacy data protection program, security policies, and / or response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products.</p> <p>Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. Refer to our Data incident response whitepaper for more information.</p>	<p>Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)</p> <p>Customer Penetration Testing</p> <p>Data Incidents (Cloud Data Processing Addendum)</p>
8.	Matters concerning the security management level of the cloud service provider	<p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.</p> <p>The confidentiality and security of information when using a cloud service consists of two key elements:</p> <p><u>(1) Security of Google's infrastructure</u></p> <p>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p>	<p>Confidentiality</p> <p>Data Security; Google's Security Measures (Data Processing and Security Terms)</p>



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

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.</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">• <u>Encryption at rest</u>. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page.• <u>Encryption in transit</u>. 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 on the Google Cloud Encryption in transit page. <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</p>	



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>data. Information on Google's security products is available on our Cloud Security Products page.</p> <p>(c) <u>Security resources</u></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none">• Security best practices• Security use cases• Security blueprints	
9.	Security requirements such as information protection obligations and service continuity	<p><u>Security requirements</u></p> <p>Refer to Row 8.</p> <p><u>Service Continuity</u></p> <p>The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.</p> <p>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.</p> <p>Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations.</p> <p>In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications.</p>	Services
10.	Retains the right to terminate the contract in the event that the service may be adversely affected	Regulated entities can elect to terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
11.	Right to monitor service level (SLA) and corrections	<u>Monitoring</u>	



#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<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, including availability and uptime of the services. 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). <p><u>Corrections</u></p> <p>If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.</p>	<p>Ongoing Performance Monitoring</p> <p>Services</p>
12.	Customer information protection and confidentiality	Refer to Row 8.	N/A
13.	Data destruction upon termination of subcontract	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper .	Deletion on Termination (Cloud Data Processing Addendum)
14.	Compliance with applicable laws and reporting obligations	<p><u>Compliance</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><u>Reporting</u></p> <p>Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis.</p>	<p>Representations and Warranties</p> <p>Significant Developments</p>



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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 at our Incidents & the Google Cloud dashboard page.</p> <p>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 Data incident response whitepaper.</p>	Data Incidents (Cloud Data Processing Addendum)
	b. Additional items		
15.	Location where information processing entrusted by financial companies is actually performed	<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 Google Cloud services can be deployed is available on our Global Locations page.- Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. <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. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <ul style="list-style-type: none">• 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.	<p>Data Transfers (Cloud Data Processing Addendum)</p> <p>Data Security; Subprocessors (Cloud Data Processing Addendum)</p> <p>Data Location (Service Specific Terms)</p>
16.	Matters regarding contingency plans, including access to data in the event of a service outage	Contingency Plans	



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> <p><u>Access to data</u></p> <p>Refer to Row 17.</p>	<p>Business Continuity and Disaster Recovery</p> <p>N/A</p>
17.	Support obligation and transition plan for transfer of consignment work to another service provider or financial company	<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> <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.</p> <p>Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.</p>	<p>Data Export (Cloud Data Processing Addendum)</p> <p>Transition Assistance</p>
18.	Measures for important situations such as merger or division, transfer of contracts, or subcontracting	<p><u>Mergers and divisions</u></p> <p>Google will provide advance notice to you if it experiences a relevant change in control.</p> <p>In addition, regulated entities can terminate our contract with advance notice for change of control.</p> <p><u>Important situations</u></p>	<p>N/A</p>



Financial Supervisory Service - Regulation on Supervision of Electronic Finance

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.</p> <p><u>Subcontracting</u></p> <p>Refer to Rows 19- 20 below.</p>	
19.	Matters requiring the consent of the financial company, such as subcontracting or change of subcontract	<p>Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities 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.	Subcontracting; Google Subcontractors
20.	Management and supervision duties of cloud service providers related to subcontracting	<p>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.</p> <p>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.</p>	Google Subcontractors