Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

This document is designed to help banks supervised by the FSC ("**regulated entity**") to consider the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (the "**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on Article 10, Article 18(6), Article 19-1 and Article 19-2 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
Article 10			
1	A financial institution's outsourcing agreement shall specify the following:		
2	10.1 The scope of outsourcing and the responsibilities of service provider.	The GCP services are described on our services summary page. The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	Definitions
3	10.2 A provision requiring the service provider to comply with Article 21 herein.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
4	10.3 Consumer protection, including the confidentiality of customer data and adoption of security measures.	The security of a cloud service consists of two key elements: 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 Google recognizes that you expect independent verification of our security, privacy and compliance controls. Refer to Row 9 on the third party audit reports we maintain. Security of your data and applications in the cloud	Data Security; Security Measures (Cloud Data Processing Addendum)

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			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 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. (b) Security resources Google also publishes guidance on: • Security best practices • Security use cases	
5	10.4	The service provider is required to carry out consumer protection, risk management, and internal control and internal audit in accordance with its standard operating procedures established under the supervision of the financial institution.	Refer to Row 9 for more information on the third party audit reports that Google provides.	N/A
6	10.5	Consumer dispute resolution mechanism, including the timetable and procedure for handling dispute and remedial measures.	Given the nature of the services Google does not have direct interactions with the regulated entities customers.	N/A
7	10.6	Management of service provider's employees, including employee recruitment, promotion, performance review and discipline.	Regulated entities can operate the services independently without action by Google personnel. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the services, given the one-to-many nature of the services, there are no Google personnel dedicated to delivering the services to an individual customer.	N/A
8	10.7	Material events that lead to the termination of outsourcing agreement with the service provider, including a provision on termination or revocation of the agreement if so instructed by the competent authority.	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.	Termination for Convenience
9	10.8	The service provider agrees to let the competent authority and Central Bank of China access relevant data or reports and conduct financial examination with respect to the outsourced items, or provide relevant data or reports within a prescribed time period under the order of the competent authority or the Central Bank of China.	Access by supervisory authorities 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. This includes access to Google's premises used to provide the Services to conduct an on-site audit. Audit reports	Regulator Information, Audit and Access, Certifications and Audit Reports

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 You can review Google's current certifications and audit reports at any time.	
10	10.9 The service provider shall not use the name of the outsourcing financial institution in the course of handling the outsourced items, nor shall the service provider make untruthful advertising or charge the customers any fees when conducting marketing of loan service.	Trademarks and logos Google will not use your brand features without your prior approval or use your data for any Google products, services or advertising. Fees Refer to your Google Cloud Financial Services Contract	Marketing and Publicity Payment Terms
11	10.10 The service provider is required to inform the financial institution where the outsourced operation involves any material irregularities or deficiencies.	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 on our Incidents & the Google Cloud dashboard page.	Significant Developments
12	10.11 Other agreements.		
13	The financial institution shall provide in the agreement requiring the service provider not to subcontract the outsourced operation unless with its written consent. The outsourcing agreement should specify the scope, limitations or conditions for subcontracting by service provider. The provisions in this article shall apply to the subcontracting agreement between the service provider and its subcontractor.	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: • 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

Taiwan FSC Outsourcing Regulations

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).	
14	Where the outsourcing agreement or sub-contracting agreement does not conform to the provisions in the Regulations herein, the financial institution may continue its outsourcing activity under the existing agreement until it expires. However if such outsourcing agreement does not have an expiration date, the financial institution shall remedy the nonconformities within six (6) months from the date the Regulations are promulgated, or else upon which the agreement expires automatically.	This is a customer consideration.	N/A
Article 18			
15	6. Where the financial institution is unable to acquire the letter of consent as described in the preceding paragraph from the foreign competent authority where the service provider is located, it shall submit the following documents:		
16	(1.) A letter of consent from the service provider, agreeing that where necessary, a person designated by the financial institution may examine the outsourced items. The aforesaid designated person may also be assigned by the competent authority at the expense of the financial institution.	Refer to Row 9 for more information on the audit, access and information rights Google grants to regulated entities, supervisory authorities and both their appointees.	N/A
17	(2.) The evaluation on internal control principles and operating procedure of the service provider.	Refer to Row 9 for more information on the third party audit reports that Google provides.	N/A
18	(3.) The legal opinion indicates the protection of customer data where the service provider is located is not below the condition in Taiwan.	Google will comply with all national data protection regulations applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum. If you would like more information about data protection in the different locations where the services are available, please contact your Google Cloud account representation.	N/A
19	(4.) The financial statements of service provider audited and attested by a CPA for the most recent fiscal year.	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.	N/A

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
20	(5.) A statement issued by the service provider certifying that no violation on customer interests, personnel malpractice, information and technology security and other occurrences that have impact on sound business operation in the last three years.	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 on our Incidents & the Google Cloud dashboard page. 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. If you would like more information about this requirement, please contact your Google Cloud account representation. Google can provide a letter confirming that it has been free of incidents of employee fraud, information or communication security breach or other incidents that result in damage to the interest of customers or adversely affect customers, for the last three years.	N/A
Article 19-1			
21	A financial institution shall comply with the following rules when its outsourced operations involve cloud-based services:		
22	1. The financial institution shall ensure proper control of operational risks and fully evaluate the risks of service provider. It shall adopt appropriate risk management and control measures to ensure the quality of outsourced operations. It shall also pay attention to proper diversification of operations outsourced to cloud service providers.	Refer to Row 43 and 44 for further information on risk assessment and management.	N/A
23	2. The financial institution is ultimately responsible for the supervision of cloud service providers and it should have the professional skills and resources to supervise the cloud service providers' execution of outsourced operations. It may also request professional third parties to assist in their supervision.	This is a customer consideration.	N/A
24	3. The financial institution shall ensure that it, the competent authority, the Central Bank, or their designated representatives have access to related information on the outsourced operations executed by cloud service providers, including the audit report of customer information relevant systems, and on-site audit right.	Refer to Row 9 for more information on the access rights granted to the regulated entity, supervisory authority and the third party audit reports that Google provides.	N/A
25	4. The financial institution may appoint an independent third party with expertise in information technology at its sole discretion or in conjunction with other financial institutions that outsource to the same cloud service provider to conduct audits and the following rules shall apply:	Google facilitates audits by regulated entities and their appointed auditors. Refer to Row 9 for more information on the access rights granted to regulated entities and its appointees.	N/A

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, Google recognizes the benefits of pooled or collective audits. We would be happy to discuss this with regulated entities.	
26	(1) The financial institution shall ensure that its audit scope includes important systems and control measures related to the operations outsourced to the cloud service provider.	The regulated entity is best placed to decide what audit scope is right for their organization. Our contract does not limit regulated entities to a pre-defined audit scope.	Customer Information, Audit and Access.
27	(2) The financial institution shall evaluate the eligibility of the third party and verify that the contents of the audit report submitted by the third party meets the relevant international standards of information security.	This is a customer consideration.Refer to Row 9 for more information on the third party audit reports provided by Google. Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party.	N/A
28	(3) The third party shall conduct audit based on the scope of outsourced operations and issue the audit report.	This is a customer consideration. Refer to Row 9 for more information on the third party audit reports provided by Google. Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope.	N/A
29	5. Where the financial institution transmits and stores customer information at the cloud service provider, it shall adopt customer data encryption, tokenization, or other effective protection measures and it shall also establish appropriate encryption key management mechanisms.	The security of your data is of paramount importance to Google. 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. In addition, you can choose to use these encryption and key management tools provided by Google: • Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. • Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. • Customer-managed encryption keys for Cloud SQL and GKE persistent disks.	N/A

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud External Key Manager (beta) lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. • Key Access Justification (alpha) works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.	
30	6. The financial institution shall retain complete ownership of data outsourced to cloud service providers for processing. The financial institution shall ensure that the cloud service provider does not have the right to access customer data except for the execution of outsourced operations and it may not use the data for purposes outside the scope of outsourced operations.	Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Data access and use 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. You can 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.	Intellectual Property Protection of Customer Data

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
31	7. In principle, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the territories of the R.O.C. If it is located outside the territories, the following rules shall apply:	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 on the Google Cloud Global Locations page. • Information about the location of Google's subprocessors' facilities is available on the Google Cloud Platform Subprocessors' page.	Data Transfers (Cloud Data Processing Addendum)
32	(1) The financial institution shall retain rights to designate the location for the processing and storage of the data.	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). 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.	N/A
33	(2) The local data protection regulations in above location shall not be lower than the requirements of the R.O.C.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. 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 of country / region.	Representations and Warranties Data Security; Subprocessors (Cloud Data Processing Addendum)
34	(3) Except with the approval of the competent authority, backups of customer important data shall be retained in the R.O.C.	Refer to Rows 31 and 32 for more information on data locations.	N/A
35	8. The financial institution shall establish appropriate emergency contingency plans to reduce the risks of service interruption due to outsourced operations When the financial institution terminates or ends the operations outsourcing, it shall ensure that the outsourced operations can be smoothly transferred to another cloud service provider or transferred back to the financial institution. It shall also ensure that the cloud service provider deletes or destroys all retained data. It shall retain records of the deletion or destruction.	Contingency plan Information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide. In particular, 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.	Business Continuity and Disaster Recovery

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Transfer 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. 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: • 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. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Transition Term Deletion on Termination (Cloud Data Processing Addendum)
Article 19-2			
36	Where a financial institution outsources operations involving cloud-based services, and outsourcing operation are material or where it outsources operations to a foreign country in accordance with Article 18, it shall submit the following documents to the competent authority for application before outsourcing:	Google recognises that use of the services could scale up over time. Regardless of how regulated entities chose to use the Services at the start of our relationship. Google will provide regulated entities with the assistance they need to review our Services.	Enabling Customer Compliance
37	1. Internal operating guidelines established in accordance with Article 4, Paragraph 2.	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.	Definitions

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
38	2. Meeting minutes containing resolutions of the board of directors, or a letter of consent signed by an officer authorized by the head office in case of the branch of a foreign bank in Taiwan.	This is a customer consideration	N/A
39	3. Regulatory compliance statement.	This is a customer consideration	N/A
40	4. Analysis of the necessity and legal compliance on outsourcing operations to cloud service providers, including compliance status evaluation to the cloud service provider with respect to the relevant customer data protection regulations.	Google will comply with all national data protection regulations applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum.	Representations and Warranties
41	5. Business plan for outsourcing. Contents include:		
42	(1) Risk assessment and management mechanisms:	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
43	A. The financial institution shall review cloud service providers to ensure the reliability and legal compliance of the services provided. The review shall include analysis of business continuity, substitutability, and concentration.	Reliability • Qualifications and competencies: 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. • Principals: Information about Google Cloud's leadership team is available on our Media Resources page. • Customer references: Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. • Performance record: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard. Business continuity, substitutability and concentration 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. Refer to Row 35 for more information on the substitutability of our services and how you can use them in your own contingency planning.	Business Continuity and Disaster Recovery
44	B. The financial institution should have the expertise and resources to monitor the performance of cloud service providers with regard to outsourced operations.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.	Ongoing Performance Monitoring

Taiwan FSC Outsourcing Regulations

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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).	
45	(2) Information security and management:	Refer to Row 4 for more information on information security and management.	N/A
46	A. Description of measures taken by financial institution with regard to the encryption, encryption tokenization, key storage, data transmission and segmentation, and ownership of data.	Refer to Row 29 for more information on encryption.	N/A
47	B. The management policies with regard to the location of data storage, including description of relevant local legal, political, and economic stability assessments for data processing and storage in a foreign country and description of data backup and the data can be accessed by financial institutions at all times.	Location Refer to Row 31 for more information on data location. Data Access Regulated entities may access their data on the services at any time.	N/A Regulator Information, Audit and Access Customer Information, Audit and Access
48	(3) The scope and method for the financial institution, the competent authority, the Central Bank, or their designated persons to obtain information with regard to outsourced operations performed by the cloud service provider, including description of access to customer information, audit reports of relevant systems and measures to ensure the rights to perform on-site audits.	Refer to Row 9 for more information on the audit, access and information rights Google grants to regulated entities, supervisory authorities and both their appointee and the audit reports Google provides.	N/A
49	(4) Emergency contingency plans and exit mechanisms, including the description of financial institution retaining sufficient resources for emergency response and exit.	Refer to Row 35 for more information on information about how customers can use our Services in their own contingency and exit planning.	N/A