OJK - SEOJK21

Google Cloud Mapping

This document is designed to help commercial banks supervised by the OJK ("**regulated entity**") to consider Circular 21 of 2017 on the application of risk management in the use of information technology by commercial banks (the "**framework**") in the context of context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: 9.2.2(c) Standard Use of IT Service Provider, 9.2.3(c) Due Diligence of IT Service Provider, 9.2.3(e) Drafting Cooperation Agreement with IT Service Provider, 9.2.3(f) Special Clauses, 9.2.3(g) Use of IT Service Provider Outside the Territory of Indonesia, 9.3.3 Risk Mitigation, and 9.3.4 Other Risk Control. 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.	9.2.2.	Standard Use of IT Service Provider		
2.	9.2.2c.	standard content of cooperation agreement with IT Service Provider, including:		
3.	9.2.2c.1)	scope of work or service;	The GCP services are described on our services summary page.	Definitions
4.	9.2.2c.2)	cost and duration of cooperation agreement;	Refer to your Google Cloud Financial Services Contract.	Payment Terms; Term and Termination
5.	9.2.2c.3)	rights and obligations of the Bank as well as the IT Service Provider;	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
6.	9.2.2c.4)	guarantee on security and data confidentiality, especially data of customers. Data can only be accessed by data owner (Bank);	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security and access.	Data Security; Security Measures (Cloud Data Processing Addendum)
7.	9.2.2c.5)	service level guarantee (SLA), containing performance standards such as service level promised and performance targets;	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
8.	9.2.2c.6)	SLA is still valid if there is change of ownership both to the Bank and IT Service Provider;	The SLAs are still valid if there is a change of ownership of either party.	Change of Control
9.	9.2.2c.7)	report on results of performance monitoring of IT Service Provider associated with SLA;	You can monitor Google's performance of the Services (including the SLAs) on an ongoing 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. • 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	Ongoing Performance Monitoring

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
10.	9.2.2c.8) risk limits borne by the Bank and IT Service Provider, among others:		
11.	9.2.2c.8a) risk of changing the scope of agreement;	Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
12.	9.2.2c.8b) change of business scope and organization of IT Service Provider company;	Google will provide advance notice to you if it experiences a relevant change in control.	Change of Control
13.	9.2.2c.8c) changes in legal and regulatory aspects; and	Google appreciates 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
14.	9.2.2c.8d) legal aspects that include copyright, patent and logo or trade mark;	Google will not use your copyright, patent, trademark or logo without your prior approval.	Marketing and Publicity; Intellectual Property
15.	9.2.2c.9) approval of the Bank in writing in the event that the IT Service Provider transfers some activities (subcontracts) to subcontractors. Moreover, subcontractors must have adequate IT operating standards;	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	Google Subcontractors

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		subcontractor. 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).	
16.	9.2.2c.10) the availability of communication facilities connected to the internet as well as the security of access and transmission of data from and to Data Center and/or Disaster Recovery Center;	Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities Refer to Row 86 for information about the security of the services, including information on encryption of data at rest and in transit.	N/A
17.	9.2.2c.11) clear regulations on data backups, policies when the condition threatens the operating continuity of the bank (contingency), protection of data of the Bank (record) including hardware, software and equipment, to ensure the continuity of IT operations;	Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	N/A
18.	9.2.2c.12) the regulation of security in the transmission of source document required from and to the Data Center and/or Disaster Recovery Center. The responsible party should be covered with sufficient insurance;	Security Refer to Row 86 for more information on the security of data in transit. Insurance Google will maintain insurance cover against a number of identified risks.	N/A Insurance
19.	9.2.2c.13) willingness to be audited either by internal of the Bank, Financial Services Authority, and/or external party appointed by the Bank or by Financial Services Authority and the availability of information for inspection purposes, including access rights, logically and physically to the data managed by IT Service Provider;	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
20.	9.2.2c.14) the IT Service Provider must provide technical documents to the Bank related to the services undertaken by IT Service Provider such as the IT process flow and the Database structure;	Refer to the Google Cloud Documentation page for technical documentation about the Services.	N/A
21.	9.2.2c.15) the IT Service Provider must report any critical event that may result in financial loss and/or disrupt the smooth operation of the Bank;	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

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			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.	Data Incidents (Cloud Data Processing Addendum)
22.	9.2.2c.16)	specifically for the implementation of Data Center, Disaster Recovery Center, and Information Technology Based Transaction Processing, the IT Service Provider must submit to the Bank the latest financial statements that have been audited each year. The IT Service Provider shall deliver the results of IT audit performed by independent auditor on a regular basis to the operation of the Data Center, Disaster Recovery Center, and/or Information Technology Based Transaction Processing to Financial Services Authority through the corresponding Bank;	Financial statements You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page. Audit Reports Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google commits to comply with the following key international standards during the term of our contract with you: • 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.	N/A
23.	9.2.2c.17)	responsibility of IT Service Provider in providing qualified and competent human resources according to the services provided to ensure the operations of the Bank are guaranteed;	Refer to Rows 37 to 39 for information about Google's qualifications and competences.	N/A
24.	9.2.2c.18)	HR training plan, whether the number to be trained, training form as well as the cost required. The IT Service Provider must transfer knowledge to the Bank, so there is personnel of IT working unit in the Bank who understands the IT used by the Bank, especially about the IT process flow and Database structure of the system provided by the IT Service Provider;	Google provides documentation to explain how regulated entities and their employees can use our services. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications.	Technical Support
25.	9.2.2c.19)	ownership and license;	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications.	Intellectual Property

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
26.	9.2.2c.20)	assurance from IT Service Provider that the provision of services will still be provided to the Bank for a certain period after the implementation;	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 during and after implementation of the Services.	N/A
27.	9.2.2c.21)	change, expiration, or termination of agreement including in the event that Financial Services Authority instructs the Bank to stop the provision of IT services prior to the expiration of the term of agreement;	Change 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. Termination and expiration Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency. Termination at the instruction of the supervisory authority Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority.	Changes to Terms; Amendments Term and Termination Termination for Convenience
28.	9.2.2c.22)	sanctions and penalties against unclear reasons for the cancellation of agreement and breach of content of the agreement;	Refer to your Google Cloud Financial Services Contract.	Liability
29.	9.2.2c.23)	compliance with laws and provisions of laws and regulations in Indonesia;	Google will comply with all laws and regulations applicable to it in the provision of the Services.	Representations and Warranties
30.	9.2.2c.24)	system security standards that must be complied with by IT Service Provider;	Refer to Row 22 for information on the system security standards that Google complies with.	N/A
31.	9.2.2c.25)	service level standards that must be complied with by IT Service Provider;	The SLAs are available on our Google Cloud Platform Service Level Agreements page.	Services
32.	9.2.2c.26)	standard report on performance monitoring of IT Service Provider; and	Refer to Row 9 for information about how you can monitor Google's performance of the service.	N/A

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
33.	9.2.2c.27)	document storage agreement standard (escrow agreement).	Refer to Row 80 for information on escrow agreements.	N/A
34.	9.2.3c.	Due Diligence of IT Service Provider		
35.		Due diligence needs to be performed to assess the reputation, technical capability, operational capability, financial condition, development plan, and ability to follow IT innovation in the market, in order for the Bank to be confident that the IT Service Provider is able to comply with the needs of the Bank. During due diligence, the Bank must take into account among others:	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 the information for each of the areas you need to consider in the rows that follow.	N/A
36.	9.2.3c.1)	existence and history of IT Service Provider company;	Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page.	N/A
37.	9.2.3c.2)	qualifications, background, and reputation of the owner of IT Service Provider company;	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. Background: You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. Principals: Information about Google Cloud's leadership team is available on our Media Resources page.	N/A
38.	9.2.3c.3)	other companies that use the same services from IT Service Provider as references;	Customer references: Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page	N/A
39.	9.2.3c.4)	ability and effectiveness of service delivery, including after sales support;	Service delivery Information about Google Cloud's service delivery capability and effectiveness is available on our Choosing Google Cloud page. Support The support services are described on our technical support services guidelines page.	N/A Technical Support

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
40.	9.2.3c.5)	technology and system architecture;	Information about Google Cloud's technology and systems architecture is available on our Choosing Google Cloud page.	N/A
41.	9.2.3c.6)	internal control environment, security history, and audit coverage;	Information about Google's internal control environment, security history and audit coverage is available in Google's certifications and audit reports. Refer to Row 22 for more information. You can review Google's current certifications and audit reports at any time.	N/A
42.	9.2.3c.7)	compliance with laws and provisions of laws and regulations;	Refer to Row 29 for information on compliance with laws.	N/A
43.	9.2.3c.8)	trust and success in relationship with sub contractors;	Refer to Row 15 on subcontracting.	N/A
44.	9.2.3c.9)	maintenance bond;	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.	N/A
45.	9.2.3c.10)	ability to provide disaster recovery and business sustainability;	Refer to Row 78 for information on Google's ability to provide disaster recovery and business continuity.	N/A
46.	9.2.3c.11)	application of risk management;	Information about Google's approach to risk management is available in Google's certifications and audit reports. Refer to Row 22 for more information. You can review Google's current certifications and audit reports at any time.	N/A
47.	9.2.3c.12)	report on result of inspection by independent party; and	Google's certifications and audit reports are produced following an inspection by an independent third party. Refer to Row 22 for more information. You can review Google's current certifications and audit reports at any time.	N/A
48.	9.2.3c.13)	financial condition including review of audited financial statements.	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.	N/A
49.		Due diligence performed by the Bank during the selection process must be well documented and regularly re-performed as part of the monitoring process. In performing regular due diligence, the Bank should take into account any changes or developments that have existed during the period since the last due diligence using the latest information.	This is a customer consideration.	N/A

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
50.	9.2.3e.	Drafting Cooperation Agreement with IT Service Provider		
51.		After selecting an IT Service Provider company, management shall draw up written agreement with IT Service Provider in accordance with agreement standards of the Bank. In drafting the agreement, the Bank must take into account of the followings:		
52.	9.2.3e.1)	content of the agreement is in accordance with the agreement standards of the Bank;	This is a customer consideration.	N/A
53.	9.2.3e.2)	through the process of discussion with the legal working unit; and	This is a customer consideration.	N/A
54.	9.2.3e.3)	consider the existence of special clause for termination of the agreement prior to the expiry of agreement if the IT Service Provider is defaulting.	Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
55.	9.2.3f.	Special Clauses		
56.		Special clauses shall take into account among others as follows:		
57.	9.2.3f.1)	In the agreement entered into between the Bank and IT Service Provider, special clause must be specified regarding the possibility of altering, entering into new agreement, or taking over activities organized by IT Service Provider or terminating the agreement before the expiry of the agreement. Include in this case shall be at the request of Financial Services Authority if necessary with the consideration that the operation by IT Service Provider may interfere with the performance of duties of Financial Services Authority.	Altering the agreement Refer to Row 27 for information on altering the agreement. Taking over activities organized by IT Service Provider Google will enable you to access and export your data throughout the duration of our contract and during a 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.	N/A Data Export (Cloud Data Processing Addendum)

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			• 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. Termination Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority. In addition, 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.	Termination for Convenience Transition Term
58.	9.2.3f.2)	The Bank is able to measure the risks and efficiency of the IT operation submitted to IT Service Provider so that the Bank can recognize in advance if there are conditions:		
59.	9.2.3f.2a)	worsening performance of IT services by IT Service Provider that can have significant impact on business activities of the Bank;	Refer to Row 9 for more information on how you can monitor Google's performance of the services.	N/A
60.	9.2.3f.2b)	inadequate solvency level of IT Service Provider, in the process leading to liquidation, or bankrupted by court;	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.	N/A
61.	9.2.3f.2c)	there is violation to the provisions of laws and regulations concerning Bank secrets and personal data of customers; and/or	Information about material pending legal proceedings is available on our annual reports page.	N/A
62.	9.2.3f.2d)	there are conditions causing the Bank from providing the necessary data in the framework of effective supervision by Financial Services Authority.	Nothing in our contract is intended to impede or inhibit the supervisory authority's ability to audit our services effectively. Refer to Row 19 for information about how regulated entities can provide their supervisory authority with access to their data on the services.	Enabling Customer Compliance
63.	9.2.3f.3)	In the event that Bank finds matters as referred to in item 2) then the Bank must:		

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
64.	9.2.3f.3)a)	report to Financial Services Authority at the longest of 3 (three) business days after the above conditions is known by the Bank;	This is a customer consideration.	N/A
65.	9.2.3f.3)b)	decide on follow-ups to be taken to address problems including discontinuance of IT services if necessary; and	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency.	Services Term and Termination
66.	9.2.3f.3)c)	report to Financial Services Authority promptly after the Bank terminates the use of IT services prior to the expiration of the term of agreement.	This is a customer consideration.	N/A
67.	9.2.3f.4)	To maintain the business continuity of the Bank in the event that the termination of use of IT services is performed prior to the expiry of the agreement, thus the Bank must have a tested and adequate contingency plan in force majeure.	Refer to Row 57 for more information on the assistance that Google provides to regulated entities on expiry or termination of the contract.	N/A
68.	9.2.3g.	Use of IT Service Provider Outside the Territory of Indonesia		
69.		Bank that plans the use of IT Service Provider outside the territory of Indonesia shall not impede the supervision or inspection by Financial Services Authority. Similar to the use of domestic IT Service Provider, the use of foreign IT services or located outside the territory of Indonesia must go through the same procedures shall be from due diligence, selection of IT Service Provider, contracting and supervision, but due to jurisdictional differences then there are other requirements that must be considered by the Bank. The use of IT Service Provider outside the territory of Indonesia must first obtain the approval of Financial Services Authority.	Refer to Row 19 on the audit, access and information rights Google grants to supervisory authorities. These rights apply regardless of the service location. Nothing in our contract is intended to impede or inhibit the supervisory authority's ability to audit our services effectively.	Enabling Customer Compliance; Regulator Information, Audit and Access
70.	9.3.3	Risk Mitigation		
71.		From the result of risk measurement, the Bank shall know the level of risk faced. Furthermore, the Bank must establish a strategy of Risk Mitigation in accordance with the risk level. The Risk Mitigation measure of the Bank must be effective to control the risk.	This is a customer consideration.	N/A

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
72.	9.3.3a.	Example of Risk Mitigation measures that can be performed by the Bank shall be among others implementing controls to reduce the likelihood of risk occurrence, such as:		
73.	9.3.3a.1)	adequate IT Service Provider agreement;	Refer to Rows 2 to 33 and 50 to 69 for more information on how the Google Cloud Financial Services Contract addresses the requirements for IT Service Provider agreements.	N/A
74.	9.3.3a.2)	monitoring the performance of service providers on a regular basis; and	Refer to Row 9 for more information on how you can monitor Google's performance of the service.	N/A
75.	9.3.3a.3)	selection of reliable IT Service Provider.	Refer to Row 34 to 49 for more information on the material Google makes available to assist with your due diligence.	N/A
76.	9.3.3b.	Other Risk Mitigation measures shall be to reduce the impact of losses if the identified risks shall occur such as insurance and Disaster Recovery Plan.	Disaster Recovery Plan Refer to Row 78 for information on disaster recovery planning. Insurance Refer to Row 18 for information on insurance.	N/A
77.	9.3.3c.	The Bank must ensure that the risk of dependence on IT Service Provider can be mitigated so that the Bank remains able of conducting its business if the IT Service Provider is defaulting, terminating the relationship, or in the process of liquidation. Risk Mitigation that can be performed shall include:		
78.	9.3.3c.1)	ensuring that IT Service Provider has a Disaster Recovery Plan in accordance with the type, scope and complexity of activities or services provided;	Google will implement a disaster recovery 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 disaster recovery planning is available in our Disaster Recovery Planning Guide	N/A
79.	9.3.3c.2)	actively obtaining the readiness guarantee of Disaster Recovery Plan owned by IT Service Provider such as periodic testing of the Disaster Recovery Plan;	Refer to Row 78 for information on Google's disaster recovery testing.	N/A
80.	9.3.3c.3)	having an escrow agreement for the storage of source code program, if the Bank does not have the source code of the application program organized by the IT Service Provider; and	Our services are one-to-many. This means that Google uses the same underlying technology to provide the services to all our Google Cloud customers. To ensure service continuity for all of our customers (including other regulated entities), we cannot enter	N/A

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			into source code escrow agreements with any individual customer. However, we recognize the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to Row 57 for more information about data portability and our Open Cloud page for more information on Google's approach to open source.	
81.	9.3.3c.4)	providing assurance from IT Service Provider to the Bank that the continuity of application is supported by the software developer in the event that the source code is not owned by the IT Service Provider.	Refer to Row 80 on service continuity.	N/A
82.	9.3.3d.	In the framework of guaranteeing the function and effectiveness of Disaster Recovery Plan, the Bank must develop and perform Disaster Recovery Plan testing periodically, comprehensively, and covering significant matters based on the type, scope, and complexity of activities undertaken by IT Service Provider. In addition, IT Service Provider must perform Disaster Recovery Plan testing on their own service provider for IT systems or facilities as well as processing transactions that is held without involving the Bank. Results of Disaster Recovery Plan testing by IT Service Provider shall be used by the Bank to update the Disaster Recovery Plan owned by the Bank.	Refer to Row 78 for more information on disaster recovery testing by Google and the regulated entity.	N/A
83.	9.3.4.	Other Risk Control		
84.		Although the Bank and IT Service Provider have used sophisticated system but still allow for irregularities such as human error, implementation of weak procedures and theft by staffs. The bank must ensure the existence of security controls for mitigating risk and covers matters:		
85.	9.3.4.a.	IT Service Provider must perform conduct background research of its staffs;	Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees.	Personnel Security; Security Measures (Cloud Data Processing Addendum)
86.	9.3.4.b.	ensuring the obligation of IT Service Provider to control the security of all IT facilities used and the data processed as well as information produced has been included in the agreement;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding data center and network security and data security. Security of Google's infrastructure The security of a cloud service consists of two key elements:	Data Security; Security Measures (Cloud Data Processing Addendum)

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 In addition, you can review Google's SOC 2 report. 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. • **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.	

OJK - SEOJK 21

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(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	
87.	9.3.4.c. ensuring the IT Service Provider understands and can meet the level of security required by the Bank for each type of data based on the sensitivity of data confidentiality; and	Refer to Row 86 on security managed by Google and security managed by the customer.	N/A
88.	9.3.4.d. ensuring the cost incurred for each security is proportional to the required level of security and in accordance with risk tolerance level that has been established by the Bank.	This is a customer consideration.	N/A