



OJK - POJK 38

Google Cloud Mapping

This document is designed to help commercial banks supervised by the OJK (“**regulated entity**”) to consider Regulation No. 38 of 2016 on the application of risk management in the use of information technology by commercial banks (the “**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on Article 20, “Organisation of Information Technology by the Bank and/or Information Technology Service Provider”, 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.	20(3) In the event that the organization of Information Technology of the Bank is performed by Information Technology service provider as referred to in paragraph (2), Bank shall be obligated:		
2.	20(3) a. to be responsible for the application of risk management;	This is a customer consideration.	N/A
3.	20(3) b. to have Information Technology work unit in place;	This is a customer consideration.	N/A
4.	20(3) c. to have the highest official who leads the Information Technology work unit;	This is a customer consideration.	N/A
5.	20(3) d. to be able to perform supervision of the performance of Bank activities that are organized by the service provider;	<p>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.</p> <p>Regulated entities can use the following functionality to control the Services:</p> <ul style="list-style-type: none">• 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. <p>In addition, refer to Row 7 for more information on how you can monitor Google's performance of the Services.</p>	Instructions
6.	20(3) e. to select Information Technology service provider based on cost and benefit analysis by engaging the Information Technology work unit of the Bank;	This is a customer consideration. Refer to Row 7 on Google's reputation for cloud services.	N/A
7.	20(3) f. to monitor and evaluate the reliability of Information Technology service provider periodically in respect of the performance, reputation of service provider, and continuity of service provision;	<p><u>Monitoring and continuity</u></p> <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.	Ongoing Performance Monitoring



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">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>Reputation</u></p> <ul style="list-style-type: none">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.	
8.	20(3) g. to provide access to internal auditor, external auditor, and Financial Services Authority to obtain data and information every time needed;	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
9.	20(3) h. to provide the Financial Services Authority with access to the Database in a timely manner, whether for the latest or historical data; and	Regulated entities may provide their supervisory authority with access to their data on the services at their discretion. In addition, refer to Row 8 for information about the audit, access and information rights Google provides to supervisory authorities.	Regulator Information, Audit and Access
10.	20(3) i. to ensure that the Information Technology service provider:		
11.	20(3) i. 1. has in place reliable experts supported by certificate of competency academically and/or professionally in accordance (with the need for the organization of Information Technology;	Refer to Row 7 on Google's reputation.	N/A
12.	20(3) i. 2. applies the principle of Information Technology control adequately as proven with the result of audit performed by independent party;	Google recognizes that regulated entities need to review our operations and internal controls for the services as part of their risk assessment. 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: <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)	Certifications and Audit Reports



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">• PCI DSS• SOC 1• SOC 2• SOC 3 <p>You can review Google's current certifications and audit reports at any time.</p>	
13.	20(3) i. 3. provides access for internal auditor of the Bank, external auditor that is appointed by the Bank, Financial Services Authority, and/or other party that is authorized in accordance with the provisions of laws and regulations to perform audit in the framework of obtaining data and information required in a timely manner every time needed;	Refer to Row 8 for information on the audit, access and information rights that Google provides to regulated entities and supervisory authorities.	N/A
14.	20(3) i. 4. states no objection in the event that the Financial Services Authority and/or other party in accordance with the law is authorized to perform audit, intends to perform audit on services activities;	Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help regulated entities review our Services, our contract does not contain pre-defined steps before regulated entities or supervisory authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Enabling Customer Compliance
15.	20(3) i. 5. as the affiliated party, maintains the security of all information including the Bank's secrets and personal data of customers;	<p>The security of a cloud service consists of two key elements:</p> <p><u>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>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>	Data Security; Security Measures (Cloud Data Processing Addendum)



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p><u>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>(a) <u>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">• 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. <p>(b) <u>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 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	
16.	20(3) i. 6. is only allowed to do subcontracting based on the approval of the Bank as proven with written document;	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.	Google Subcontractors



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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. <p>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).</p>	
17.	20(3) i. 7. reports to the Bank on any critical event that can inflict significant financial loss and/or disrupt the smooth operation of the Bank;	<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 on 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>	<p>Significant Developments</p> <p>Data Incidents (Cloud Data Processing Addendum)</p>
18.	20(3) i. 8. delivers the result of audit on Information Technology performed by independent auditor periodically to the organization of Data Center, Disaster Recovery Center, and/or Information Technology Based Transaction Processing, to Financial Services Authority through the relevant Bank;	<p>Refer to Row 12 on certifications and audit reports. You can review Google's current certifications and audit reports at any time.</p>	N/A
19.	20(3) i. 9. provides a tested and adequate Disaster Recovery Plan;	<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>	Business Continuity and Disaster Recovery
20.	20(3) i. 10. accepts possible termination of agreement prior to the expiration of term of agreement (early termination); and	<p>Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with the law.</p> <p>In addition, 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.</p>	Term and Termination



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
21.	20(3) i. 11.complies with the service level in accordance with service level agreement between the Bank and Information Technology service provider.	The SLAs are available on our Google Cloud Platform Service Level Agreements page.	Services
22.	20(4) The use of Information Technology service provider by the Bank as referred to in paragraph (3) shall be obligated to be based on a written agreement that includes at least the willingness of Information Technology service provider to organize and/or perform the matters as referred to in paragraph (3) letter i.	The use and provision of the Services is based on the Google Cloud Financial Services Contract. Refer to Rows 10 to 21 for more information about how our contract addresses the requirements of paragraph 3.	N/A
23.	20(5) Bank shall be obligated to undergo selection process in selecting Information Technology service provider with due observance of prudential principle, risk management, and based on arm's length principle, in the event that Information Technology service provider is a related party to the Bank.	This is a customer consideration.	N/A
24.	20(6) Bank shall be obligated to take particular measure in the event that the following condition occurs:		
25.	20(6) a. the performance of the organization of Information Technology by Information Technology service provider is worsen that may have significant impacts on the business activities of the Bank;	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Services
26.	20(6) b. Information Technology service provider becomes insolvent, in the liquidation process, or declared bankrupt by the court;	Regulated entities may terminate our contract with advance notice for Google's insolvency.	Term and Termination
27.	20(6) c. violation by Information Technology service provider of the confidentiality conditions of the Bank and its obligation to keep confidential of personal data of customers; and/or	Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
28.	20(6) d. condition that causes the Bank unable to provide the required data in the framework of supervision by the Financial Services Authority.	For information about how regulated entities can provide their supervisory authority with access to their data on the services refer to Row 9. For information about how regulated entities can provide their supervisory authority with access to their data on the services.	Enabling Customer Compliance
29.	20(7) Particular action as referred to in paragraph (6) shall be, at least:		
30.	20(7) a. to report to the Financial Services Authority by no later than 3 (three) business days after the conditions as referred to in paragraph (6) are known by the Bank;	This is a customer consideration.	N/A
31.	20(7) b. to decide the follow-ups to be taken to overcome the problems including the stoppage of use of services in case required; and	If you wish to stop using our services, you can do so at any time.	Ceasing Services Use
32.	20(7) c. to report to Financial Services Authority immediately after the Bank stops the use of service prior to the expiration of the term of agreement.	This is a customer consideration.	N/A
33.	20(8) In the event that the use of Information Technology service provider or plan on the use of Information Technology service provider causes or is indicated to cause a		



OJK - POJK38

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	difficulty in the supervision performed by the Financial Services Authority, the Financial Services Authority may:		
34.	20(8) a. order the Bank to stop the use of Information Technology prior to the expiration of the term of agreement; or	Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority	Termination for Convenience
35.	20(8) b. reject the plan on the use of Information Technology service provider as submitted by the Bank.	This is a customer consideration.	N/A