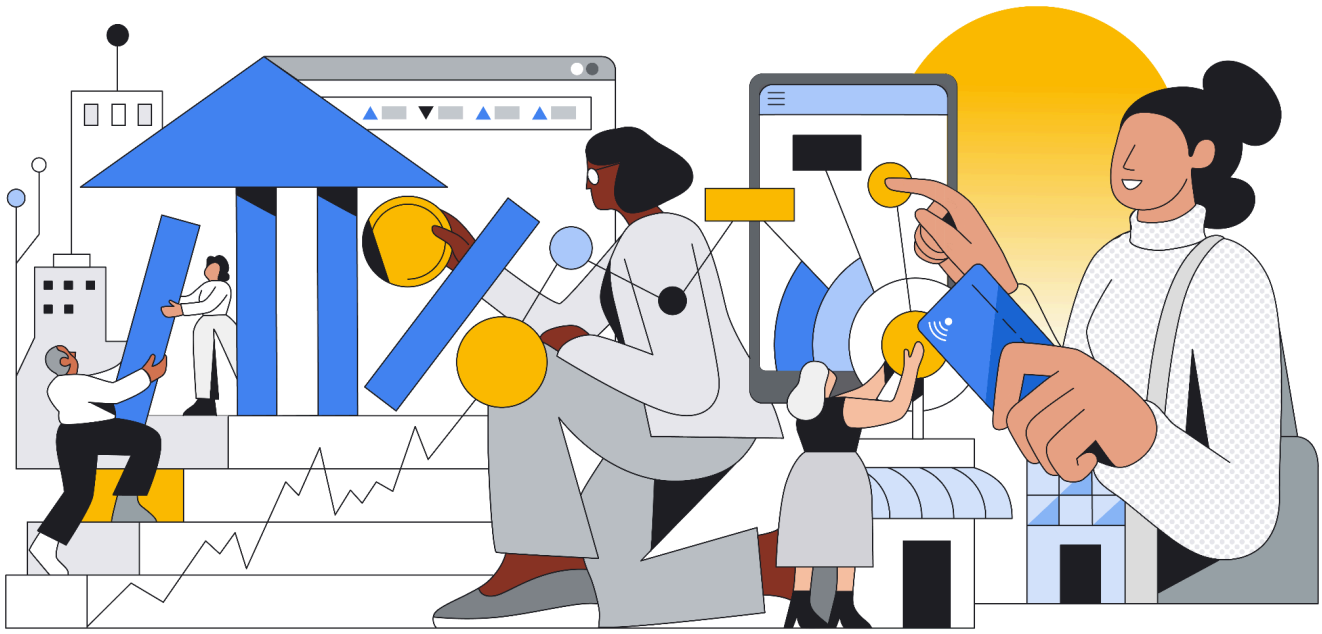
Google Cloud Whitepaper
July 2025

Indonesian Financial Services Regulations: A Guide for Institutions Using Google Cloud



Authors: Airish Mariano, Mandar Bale

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of July 2025 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Abstract

As Indonesia's financial sector increasingly adopts digital technologies, banks and financial institutions must navigate a constantly evolving regulatory framework. This guide is here to help you, as a financial institution regulated by OJK (Otoritas Jasa Keuangan, the Financial Services Authority) and BI (Bank Indonesia), confidently adopt and expand your use of Google Cloud.

This guide highlights Google Cloud's core commitment to security and compliance and details how our services align with key security and control domains typically addressed in the regulations, including Information Technology (IT) governance, risk management, cyber defense, data management, and data residency. It further presents guidance on how Google Cloud can help you comply with specific applicable requirements in the regulations and guidelines issued by the OJK and BI. By using this guide, you can learn how to leverage Google Cloud's secure infrastructure and tools, helping you meet security and regulatory goals when designing your cloud environment.

Ultimately, this resource empowers you to build a robust risk governance framework for effectively managing IT risks, strengthening cybersecurity, protecting sensitive data, and ensuring operational continuity. It is designed to accelerate your secure adoption of Google Cloud, providing the information and resources needed for enabling your regulatory compliance.

Google Cloud's Commitment to Security and Compliance

At Google Cloud, security and compliance are integral to the design and operation of our platform. We understand that for financial institutions, trust is paramount, and independent verification of security, privacy, and compliance controls is essential. Our fundamental approach is to deliver a highly secure and resilient infrastructure, complemented by a comprehensive suite of tools and services that empower you to protect your data and applications effectively.

To offer this assurance, Google Cloud undergoes regular, independent third-party audits. We are committed to adhering to key international standards that provide a robust framework for meeting the requirements of OJK and BI on financial institutions. 11/POJK.03/2022. These include: ISO/IEC 27001 (Information Security Management Systems), which aligns with the Indonesian SNI 27001, ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (Cloud Privacy), PCI DSS, SOC 1, SOC 2, SOC 3, and ISO 42001 (Artificial Intelligence Management Systems). These certifications validate our rigorous controls over information security, cloud-specific security, privacy for personal data in the cloud, financial reporting controls, and AI management systems, establishing a credible basis for your own compliance initiatives. You can access Google's current certifications and audit reports at any time via our Compliance Reports Manager, which provides streamlined, on-demand access to these crucial compliance resources.

Key Regulations to Consider for Cloud Adoption

Indonesia's financial sector regulations underscore stringent requirements for IT governance, risk management, data protection, and consumer safeguards, particularly concerning IT outsourcing and cloud adoption. Here is a breakdown of some key regulations[1] for financial institutions to consider when using cloud services:

OJK Regulations

- **11/POJK.03/2022 on Information Technology Implementation by Commercial Banks.** This regulation comprehensively governs IT planning, risk management, cybersecurity, data localization, and IT outsourcing for banks. Banks are responsible for retaining ultimate IT risk management, conducting due diligence, and overseeing outsourced IT effectively.
- **21/SEOJK.03/2017 on the Application of Risk Management in the Use of Information Technology by Commercial Banks.** This circular provides detailed guidance on implementing IT risk management for banks, specifically for outsourcing arrangements. Banks must ensure outsourcing agreements define clear responsibilities, service levels, and robust oversight mechanisms. This circular is the implementing regulation for OJK Regulation 38/POJK.03/2016 (and its amendments) which has been replaced by OJK Regulation 11/POJK.03/2022. The circular remains in effect to the extent it does not contradict with the provisions under OJK Regulation 11/POJK.03/2022.
- **3/POJK.03/2024 on the Organization of Technological Innovation in the Financial Sector.** This regulation governs financial technology innovation and its related frameworks within the financial services sector. Financial institutions using fintech are responsible for robust risk management, consumer protection, and data security throughout the innovation lifecycle.
- **4/POJK.05/2021 on the Application of Risk Management in the Use of Information Technology by Non-Bank Financial Institutions.** This regulation addresses the application of IT risk management for non-bank financial institutions. Non-bank financial institutions must implement robust IT risk management frameworks and oversee outsourced IT activities.
- **22/POJK.03/2023 on Consumer and Public Protection in the Financial Services Sector.** This regulation aims to enhance consumer protection across the financial services sector, covering various aspects including data privacy and fair treatment. Financial institutions must ensure outsourced IT activities uphold strict consumer protection and data privacy, maintaining full accountability.

BI Regulations

- **22/23/PBI/2020 on Payment System.** This regulation governs the overall payment system in Indonesia, emphasizing reliability, security, and efficiency. Payment system operators are responsible for ensuring the reliability, security, and efficiency of their IT systems for payment processing.
- **23/6/PBI/2021 on Payment Service Providers.** This regulation provides specific guidelines and licensing requirements for Payment Service Providers (PJPs). PJPs must implement secure and reliable systems, including fraud management, with strict oversight of supporting providers.
- **23/7/PBI/2021 on Payment System Infrastructure Providers.** This regulation focuses on Payment System Infrastructure Providers (PIPs) and their role in maintaining payment system stability. PIPs are

[1] *This is not an exhaustive list. We encourage all customers to actively engage with their legal and compliance teams to address all other applicable laws and regulations specific to their operations.*

primarily responsible for infrastructure stability, IT system capability, risk management, and operational continuity.

Underpinning consumer data protection

- **Law No. 27 of 2022 on Personal Data Protection, also known as PDP Law.** While not issued by OJK or BI, this comprehensive law governs personal data processing across all Indonesian sectors, defining rights for data subjects and obligations for data controllers and processors. Financial institutions, as Data Controllers, are primarily responsible for lawful, transparent, and accountable personal data processing and ensuring third-party adherence.

Google Cloud provides the technical capabilities and a shared responsibility model that can help your organization meet these regulatory expectations. The following sections provide more information on how we can support your journey to regulatory compliance.

Enabling Your Compliance

The OJK and BI regulations generally place significant emphasis on key aspects of IT governance and IT service provider management, risk management and compliance, cyber defense and security, data management and governance, and data residency and cross-border transfers. Google Cloud offers a comprehensive set of services and features that directly align with these core domains, enabling you to address the regulations' mandates effectively.

Addressing shared aspects of the regulations

IT Governance and IT Service Provider Management

The regulations underscore the importance of banks' effective IT governance and risk management when engaging with IT service providers. Google Cloud operates on a transparent model where customers retain control over their services. You determine which services to utilize, how to configure them, and their specific purpose, ensuring your organization maintains oversight of relevant activities.

- **Control and Management Tools:** You can manage your Google Cloud resources using the Cloud Console (a web-based graphical user interface), the gcloud Command Tool (our primary command-line interface for Google Cloud), and Google APIs (Application Programming Interfaces that provide programmatic access to Google Cloud). These interfaces enable granular control over your cloud environment.
- **Performance Monitoring and Transparency:** You can continuously monitor Google's performance of the services, including adherence to Service Level Agreements (SLAs). The Service Health Dashboard provides real-time status information on Google Cloud services. Personalized Service Health filters disruptive events relevant to your projects, helping you assess impact and maintain business continuity. **Google Cloud Operations** (which includes Cloud Logging, Cloud Monitoring, and Cloud Trace) offers an integrated solution for monitoring, logging, and diagnostics, providing deep insights into your applications running on Google Cloud, including service availability and uptime.
- **Access Transparency:** This Google Cloud feature provides logs of actions taken by Google personnel concerning your data. Log entries include the affected resource, the time of action, the reason for the action (e.g., the case number associated with a support request), and data about the Google personnel involved (e.g., their location). This offers visibility and auditability into Google's operations, directly supporting your oversight requirements for IT service providers. Additionally, Access Approval 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.

Risk Management and Compliance

The regulations also highlight the increased IT risk exposure for banks, including cyber incidents and data leakage. Google Cloud understands your need to conduct due diligence and perform comprehensive risk assessments before adopting our services.

- **Due Diligence and Third-Party Risk Management (TPRM):** We provide extensive documentation and resources to support your due diligence processes. Google collaborates with independent TPRM providers who conduct regular assessments of Google Cloud's platform and services. These assessments examine security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, and SOC2. The resulting independent audit reports can help streamline and accelerate your internal risk assessment processes. For more information, refer to our Google Cloud Third Party Risk Management Resource Center.
- **Proven Experience and Corporate Information:** With over a decade of providing cloud services, Google Cloud supports customers across diverse sectors globally, including financial services. Our Financial Services Cloud Blog and Financial Services solutions page detail how financial institutions leverage Google Cloud to drive business transformation, foster data-driven innovation, and meet security and compliance objectives. Information about Google's corporate history, mission, business model, strategy, organizational policies (including our Code of Conduct) and audited financial statements are available on Alphabet's Investor Relations page. You can also review information about Google's historical service performance on our Google Cloud Service Health Dashboard.

Cyber Defense and Security

Another significant focus is on strengthening IT organization management to mitigate risks, particularly cyber incidents. Google Cloud provides robust cybersecurity capabilities integrated throughout our infrastructure and services.

- **Security of Google's Infrastructure:** Google manages the security of our infrastructure, encompassing the hardware, software, networking, and facilities that support the Services. We provide detailed information about our security practices, including our infrastructure security page, security whitepaper, infrastructure security design overview page, and security resources page. To help protect customer data, we run an industry-leading information security operation that combines stringent processes, an expert incident response team, and multi-layered information security and privacy infrastructure.
- **Security of Your Data and Applications:** You define the security measures for your data and applications within the cloud. Google proactively takes steps to assist you, including **encryption at rest** (enabled by default with no additional action required from you, as detailed on the Google Cloud Encryption at rest page) and **encryption in transit** (encrypting and authenticating all data when it moves outside physical boundaries not controlled by Google or on behalf of Google, as detailed on the Google Cloud Encryption in transit page). Our SOC 2 report attests to the design and operating effectiveness of controls related to the Trust Services Criteria of security, availability, processing integrity, confidentiality, and privacy. It specifically covers Google's controls that protect customer data within the Google Cloud Platform system, including logical and physical access, system operations, and change management.
- **Security Products and Resources:** You can enhance and monitor your data's security using a wide

range of Google's security products and services:

- Security Command Center (SCC) provides a centralized platform for managing security and risk across your cloud environment. It offers capabilities to prevent, detect, and respond to security issues by integrating services that address vulnerability detection, threat detection, compliance monitoring, and security posture management. SCC helps you gain comprehensive visibility into your assets, identify misconfigurations and threats, and offers tools for effective remediation to strengthen overall cloud security.
- Google Cloud Armor offers robust, global protection against DDoS attacks and provides Web Application Firewall (WAF) services with customizable rules, helping ensure the availability and security of your internet-facing applications.
- reCAPTCHA Enterprise protects websites and applications from fraudulent activity and spam by distinguishing between human users and bots.
- Google Threat Intelligence capabilities leverage Google's vast global network and security expertise to provide customers with continuously updated, actionable insights into emerging threats, enabling proactive defense against sophisticated attacks.
- Google Security Operations unifies security operations with AI-powered analytics to accelerate threat detection, investigation, and response, ultimately strengthening customer security posture.
- Mandiant Cybersecurity Consulting offers strategic services like cyber defense transformation and incident response, enabling customers to proactively enhance their defenses and effectively respond to evolving threats.

- **Operational Resilience:** Google Cloud's disaster recovery (DR) and operational resilience are tightly integrated; DR is a core part of our holistic resilience strategy, ensuring rapid service and data restoration for business continuity. We achieve this through continuous, automated disaster readiness and recovery for all Google's systems and data. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper further elaborates on the importance of resilience, and we also provide guidance on how you can leverage Google Cloud's inherent reliability features (like zones, regions, and location-scoped resources) and architectural best practices to build robust DR solutions for your cloud infrastructure.

Data Management and Governance

The regulations stress the importance of preventing customer personal data leakage and ensuring appropriate data management practices. Google Cloud offers services that facilitate robust data governance, protection, and responsible data processing.

- **Data Access and Use Commitments:** Google commits to accessing or using your data solely to provide the Services you ordered and will not use it for any other Google products, services, or advertising.
- **Subcontractor Compliance:** We require our subcontractors to meet the same high standards, ensuring they comply with our contract with you and only access and use your data as required to perform their subcontracted obligations.
- **Data Protection Laws & Regulations:** Google complies with all national data protection regulations applicable to it in the provision of the Services, as addressed in the Cloud Data Processing Addendum. We are committed to upholding robust data privacy and security measures, including strong contractual commitments, encryption, and transparent practices, to help customers comply with Indonesia's Personal Data Protection Law.
- **Data Loss Prevention: Sensitive Data Protection** helps you discover, classify, and protect sensitive data across your Google Cloud environment, preventing unauthorized access and leakage. It can scan various data sources for sensitive information, such as national identification numbers, credit card numbers, and other personally identifiable information (PII).

- **Secure Data Storage and Analytics: Cloud Storage** provides highly durable, available, and secure object storage for all your data, with options for encryption at rest and in transit. **BigQuery**, our fully managed, petabyte-scale data warehouse, offers robust security features including column-level encryption, row-level security, and auditing capabilities, enabling secure data analytics while maintaining compliance. Services like **Dataproc** allow for secure and compliant processing of large datasets.

Data Residency and Cross-Border Transfers

Certain regulations, such as 11/POJK.03/2022, place specific emphasis on data localization for Electronic Systems and the processing of IT-Based Transactions, often requiring regulatory approval for such transactions. Google Cloud provides choices and controls to help you meet these critical requirements.

- **Region Selection:** Google Cloud offers regions globally, including the **Jakarta (asia-southeast2)** region in Indonesia. You maintain control over where your data at rest is stored by selecting the specific Google Cloud region or multi-region for your resources, as detailed on our Global Locations page. This capability allows you to deploy your electronic systems and store your data within Indonesia or other suitable regions, supporting data residency requirements. Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.
- **Data Location and Encryption:** All data stored in Google Cloud is encrypted at rest and in transit. You retain control over your data's location, and our contractual terms specify our commitments regarding data residency and data handling. For particular services, you can configure data residency policies to ensure data remains within designated geographic boundaries, minimizing the need for cross-border transfers where prohibited. More information is available in our Google Cloud Trust Center.
- **Data Incident Response:** 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 process. To assist customers with their own incident response, Google's notification will describe the nature of the data incident, including impacted customer resources; measures Google has taken or plans to take; recommended customer actions; and details of a contact point for more information.
- **Controlled Approach to Government Data Requests:** Google has a rigorous and transparent process for handling government requests for cloud customer data, emphasizing a strong commitment to data protection by carefully evaluating each request, challenging overly broad demands, and providing robust security and privacy controls to customers.
- **Compliance with PDP Law:** You should also review Google Cloud's whitepaper on PDP Law (Indonesia) which would help you understand the PDP Law and how Google Cloud implements data privacy and security capabilities to store, process, maintain, and secure customer data in a way that aids customers in meeting their PDP Law obligations.

Compliance with 11/POJK.03/2022 and 21/SEOJK.03/2017 in the context of Google Cloud

POJK 11/2022 sets the primary IT framework for banks, while SEOJK 21/2017 details risk management for using information technology for banks. Market insights indicate that both POJK 11/2022 and SEOJK 21/2017 are important for navigating the regulatory approval process for the use of cloud services. As such, we provide further guidance[2] on how Google Cloud can help you address the applicable requirements under these regulations:

[2] *To ensure comprehensive compliance, it is the financial institution's responsibility to understand and meet all applicable regulatory requirements beyond those outlined here.*

11/POJK.03/2022 - Articles 29 to 32

#	Framework Reference	Google Cloud Commentary
Article 29 mandates the banks' supervision, risk management and policies for IT outsourcing.		
1	(2) Banks that use IT service providers as referred to in paragraph (1) must possess the ability to supervise the implementation of Banks activities organized by IT service providers.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control the Services: • **Cloud Console:** A web-based graphical user interface that customers can use to manage their Google Cloud resources. • **gcloud Command Tool:** A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. • **Google APIs:** Application programming interfaces which provide access to Google Cloud.
2	(3) Banks must have policies and procedures for the use of IT service providers as referred to in paragraph (1) that at least contain:	
3	(3) a. identification process of the needs of IT service providers;	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 below. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page. Technical capacity / service delivery / reputation 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. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support
4	(3) b. selection process of IT service providers;	
5	(3) c. procedures for cooperation with IT service providers;	
6	(3) d. the risk management process of the use of IT service providers; and	

#	Framework Reference	Google Cloud Commentary
		data-driven innovation, customer expectations, and security & compliance. You can review information about Google's historic performance of the services on our Google Cloud Service Health Dashboard. Corporate information Information about Google's corporate history is available on Alphabet's Investor Relations page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. To obtain other information about Google Cloud's financial information you may need, please contact [the Google Cloud sales team that you have been communicating with]. You can review Google's audited financial statements on Alphabet's Investor Relations page. You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct, which addresses conflicts of interest. To obtain other corporate information you may need, please contact [the Google Cloud sales team that you have been communicating with]. People Information about Google Cloud's leadership team is available on our Media Resources page. To obtain other information about Google Cloud's leadership team you may need, please contact [the Google Cloud sales team that you have been communicating with]. Risks Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page. Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page. Compliance As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards

#	Framework Reference	Google Cloud Commentary
		from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information. ** Please also review our commentary on Article 9.2.3c of OJK Circular 21/SEOJK.03/2017 which elaborates further on the subject of due diligence for cloud providers.*
7	(3) e. procedures for assessing the performance and compliance of IT service providers.	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 Service Health Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud Monitoring is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, 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).
Article 30 sets out requirements for banks on governing IT service provider engagement procedures. **Please also review our commentary on Article 9.2.2(c), Article 9.2.3(e) and Article 9.2.3(f) of OJK Circular 21/SEOJK.03/2017 below which provides further requirements for agreements with a cloud provider.*		
8	(3) Banks in engaging in a cooperative relationship with IT service providers as referred to in Article 29 paragraph (3) letter c must have a cooperation agreement with IT service providers, with due regard to at least the following:	
9	(3) a. qualifications and competencies of human resources owned by IT service providers;	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.

#	Framework Reference	Google Cloud Commentary
10	(3) b. commitment of IT service providers in maintaining the confidentiality of data and/or information of Banks as well as of Banks' customers;	Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality.
11	(3) c. commitment of IT service providers to periodically submit results of IT audits which are conducted by independent auditors for the provision of IT services to Banks;	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 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.
12	(3) d. transfer of part of the activities or subcontracts by IT service providers shall be undertaken with the approval of Banks as proven by written documents;	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. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting arrangement. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice.
13	(3) e. reporting mechanism of critical events by IT service providers to Banks;	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 Service Health Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates.

#	Framework Reference	Google Cloud Commentary
		You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud Monitoring is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, 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).
14	(3) f. termination mechanism of the cooperation agreement if there is a termination of agreement before the term of the agreement expires;	Regulated entities can elect to terminate our contract for convenience with advance notice, including: -if necessary to comply with law; and -if directed by a supervisory authority; and -if Google increases the fees. In addition, regulated entities can terminate our contract with advance notice: -for Google's material breach after a cure period; and -for change of control; and -for Google's insolvency
15	(3) g. fulfillment of laws and regulations on the provision of IT services by IT service providers;	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.
16	(3) h. willingness of IT service providers to fulfill the obligations and/or requirements contained in the cooperation agreement; and	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.
17	(3) i. willingness of IT service providers to provide access to the Financial Services Authority and/or other authorized parties to conduct assessments on the provision of IT services provided in accordance with provisions of laws and regulations.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.
Article 31 - 32 mandate that banks reassess IT service provider materiality after significant organizational changes.		
18	32.(1) In the event of the following conditions: (see list below) Banks must take certain actions.	
19	(1) a. results of the materiality reassessment as referred to in the Article	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated

#	Framework Reference	Google Cloud Commentary
	31 indicates that the performance of IT service providers has the potential to be ineffective;	entities may claim service credits.
20	(1) b. deteriorating performance in the IT organization by IT service providers which has the potential to cause and/or result in a significant impact on the business activities and/or operations of Banks;	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.
21	(1) c. IT service providers become insolvent, are in the process of being liquidated, or have been declared bankrupt by the court;	Regulated entities can elect to terminate our contract for convenience with advance notice, including: -if necessary to comply with law; and -if directed by a supervisory authority; and -if Google increases the fees. In addition, regulated entities can terminate our contract with advance notice: -for Google's material breach after a cure period; and -for change of control; and -for Google's insolvency
22	(1) d. there is a violation by IT service providers against provisions of laws and regulations on Banks secrecy and/or customers' personal data;	Regulated entities can elect to terminate our contract for convenience with advance notice, including: -if necessary to comply with law; and -if directed by a supervisory authority; and -if Google increases the fees. In addition, regulated entities can terminate our contract with advance notice: -for Google's material breach after a cure period; and -for change of control; and -for Google's insolvency
23	(1) e. there are conditions that cause Banks to be unable to provide data required for supervision by the Financial Services Authority; and/or	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.
24	(1) f. there are other conditions that lead to the disruption or cessation of the provision of IT services from IT service providers to Banks	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.

21/SEOJK.03/2017 - Articles 9.2.2(c), 9.2.3(c), 9.2.3(e), 9.2.3(f), 9.2.3(g), 9.3.3-4

#	Framework Reference	Google Cloud Commentary
9.2.2(c). Standard Use of IT Service Provider		
1	9.2.2c. standard content of cooperation agreement with IT Service Provider, including:	
2	9.2.2c.1) scope of work or service;	The Google Cloud services are described on our services summary page.
3	9.2.2c.2) cost and duration of cooperation agreement;	Refer to your Google Cloud Financial Services Contract.
4	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.
5	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.
6	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.
7	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.
8	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 Monitoring is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud. 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).
9	9.2.2c.8) risk limits borne by the Bank and IT Service Provider, among others:	
10	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.

#	Framework Reference	Google Cloud Commentary
		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.
11	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.
12	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.
13	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.
14	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 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).
15	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 79 for information about the security of the services, including information on encryption of data at rest and in transit.
16	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	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.

#	Framework Reference	Google Cloud Commentary
	continuity of IT operations;	
17	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.
18	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.
19	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.
20	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 Service Health Dashboard. 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.
21	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

#	Framework Reference	Google Cloud Commentary
		You can review Google's current certifications and audit reports at any time.
22	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 35 to 37 for information about Google's qualifications and competences.
23	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.
24	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.
25	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.
26	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.
27	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.
28	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.

#	Framework Reference	Google Cloud Commentary
29	9.2.2c.24) system security standards that must be complied with by IT Service Provider;	Refer to Row 21 for information on the system security standards that Google complies with.
30	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.
31	9.2.2c.26) standard report on performance monitoring of IT Service Provider; and	Refer to Row 8 for information about how you can monitor Google's performance of the service.
32	9.2.2c.27) document storage agreement standard (escrow agreement).	Refer to Row 74 for information on escrow agreements.
9.2.3(c). Due Diligence of IT Service Provider		
33	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.
34	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.
35	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. To obtain other information about Google Cloud's leadership team you may need, please contact [the Google Cloud sales team that you have been communicating with].
36	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
37	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.

#	Framework Reference	Google Cloud Commentary
38	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.
39	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.
40	9.2.3c.7) compliance with laws and provisions of laws and regulations;	Refer to Row 28 for information on compliance with laws.
41	9.2.3c.8) trust and success in relationship with sub contractors;	Refer to Row 14 on subcontracting.
42	9.2.3c.9) maintenance bond;	You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.
43	9.2.3c.10) ability to provide disaster recovery and business sustainability;	Refer to Row 72 for information on Google's ability to provide disaster recovery and business continuity.
44	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 21 for more information. You can review Google's current certifications and audit reports at any time.
45	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 21 for more information. You can review Google's current certifications and audit reports at any time.
46	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. To obtain other information about Google Cloud's financial information you may need, please contact [the Google Cloud sales team that you have been communicating with].
47	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.
9.2.3(e). Drafting Cooperation Agreement with IT Service Provider		
48	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:	

#	Framework Reference	Google Cloud Commentary
49	9.2.3e.1) content of the agreement is in accordance with the agreement standards of the Bank;	This is a customer consideration.
50	9.2.3e.2) through the process of discussion with the legal working unit; and	This is a customer consideration.
51	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.
9.2.3(f). Special Clauses		
52	Special clauses shall take into account among others as follows:	
53	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. Migrate to Containers 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.
54	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:	
55	9.2.3f.2a) worsening performance of IT services by IT Service Provider that can have significant impact on business	Refer to Row 9 for more information on how you can monitor Google's performance of the services.

#	Framework Reference	Google Cloud Commentary
	activities of the Bank;	
56	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.
57	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.
58	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.
59	9.2.3f.3) In the event that Bank finds matters as referred to in item 2) then the Bank must:	
60	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.
61	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.
62	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.
63	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 56 for more information on the assistance that Google provides to regulated entities on expiry or termination of the contract.
9.2.3(g). Use of IT Service Provider Outside the Territory of Indonesia		
64	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	Refer to Row 18 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.

#	Framework Reference	Google Cloud Commentary
	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.	
9.3.3 Risk Mitigation		
65	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.
66	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:	
67	9.3.3a.1) adequate IT Service Provider agreement;	Refer to Rows 1 to 32 and 49 to 69 for more information on how the Google Cloud Financial Services Contract addresses the requirements for IT Service Provider agreements.
68	9.3.3a.2) monitoring the performance of service providers on a regular basis; and	Refer to Row 8 for more information on how you can monitor Google's performance of the service.
69	9.3.3a.3) selection of reliable IT Service Provider.	Refer to Row 33 to 51 for more information on the material Google makes available to assist with your due diligence.
70	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.
71	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:	
72	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

#	Framework Reference	Google Cloud Commentary
73	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.
74	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 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 Modern Infrastructure Cloud page for more information on Google's approach to open source.
75	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.
76	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 72 for more information on disaster recovery testing by Google and the regulated entity.
9.3.4. Other Risk Control		
77	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:	
78	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.

#	Framework Reference	Google Cloud Commentary
79	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: 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 on the Google Cloud Encryption at rest page. 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 on the Google Cloud Encryption in transit page. (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.

#	Framework Reference	Google Cloud Commentary
		(c) Security resources Google also publishes guidance on: Security best practices Security use cases
80	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 79 on security managed by Google and security managed by the customer.
81	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.

Shared Responsibility and Shared Fate on Google Cloud

Operating in the cloud involves a shared responsibility model, where Google Cloud and our customers both play essential roles in ensuring security and compliance. Google is responsible for the security *of* the cloud, meaning we secure the underlying infrastructure, network, and foundational services that support your operations. This includes our global data centers, hardware, software, networking, and the processes and controls for maintaining these systems.

Conversely, you, the customer, are responsible for security *in* the cloud. This entails the security of your configurations within the cloud environment, the security of your applications and data, identity and access management, network configurations, and the overall security posture of your cloud deployments. Our shared fate model signifies that we succeed together; your compliance is a collective objective, and we provide the platform and tools to assist you in achieving it. While Google Cloud furnishes a secure platform and comprehensive tools, the ultimate responsibility for achieving and maintaining compliance with the Indonesian laws and regulations rests with your organization, based on your specific implementation and operational practices. For more details on this model, refer to the Shared Responsibility and Shared Fate documentation.

Partnering on Your Compliance Journey

Google Cloud is more than a technology provider; we are your partner in navigating the complexities of regulatory compliance. We are dedicated to continuously enhancing our platform and services to help financial institutions in Indonesia meet evolving requirements and innovate securely.

We encourage you to explore Google Cloud's comprehensive compliance resource center to access whitepapers, compliance guides, and detailed documentation relevant to the financial sector and data governance, including the Google Cloud Trust Center, Security section, Geography and Regions documentation, Security Best Practices, and Privacy information. For guidance on how Google Cloud can support your journey to comply with specific OJK or BI regulations, please do not hesitate to contact your Google Cloud account team. We are here to help you build and operate secure, compliant, and transformative solutions in the cloud.