HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in Indonesia

Issue 1.0

Date 2023-02-08

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing technology and services has become the norm for Indonesian financial institutions. Cloud computing brings great convenience to the development of financial institutions, but also creates a more complex business operation environment for financial institutions. In order to standardize the application of information technology in the financial industry, the Indonesian Financial Services Authority (OJK) has issued a series of regulatory provisions on the network security, information technology risk management and other aspects of Indonesian financial institutions.

As a cloud service provider, HUAWEI CLOUD is committed to helping financial customers meet these regulatory requirements, and continues to provide financial customers with cloud services and business operation environments that comply with financial industry standards. This article will describe in detail how HUAWEI CLOUD will help Indonesian financial institutions meet regulatory requirements when using cloud services.

1.2 Introduction of Applicable Indonesian Financial Regulatory Requirements

The Indonesian Financial Services Authority is the financial services regulatory authority in Indonesia, responsible for supervising and managing the IT risk management of financial institutions and nonbank financial institutions, and has promulgated relevant regulations to regulate this field.

- **Implementation of Risk Management in the use of Information Technology by Commercial Banks** (referred to as "POJK MRTI"): On December 14, 2016, the Indonesian Financial Services Authority issued this regulation, which puts forward risk management requirements for commercial banks to implement IT technology, involving requirements in multiple IT fields, such as business continuity, data security, information security, supplier requirements, etc.
- **Implementation of Risk Management in the use of Information Technology by Commercial Banks**: On June 18, 2020, the Indonesian

Financial Services Authority issued the amendment, which revised the provisions of No.38/POJK.03/2016 on data center and disaster recovery center, and put forward further requirements.

- **Implementation of Risk Management in the use of Information Technology by Commercial Banks**: On June 6, 2017, the Indonesian Financial Services Authority issued the notice on the basis of the No.38/POJK.03/2016 Provisions on the Implementation of Risk Management by Commercial Banks in the Use of Information Technology. The notice proposed risk management requirements for commercial banks to implement IT technology, involving requirements in multiple IT fields, such as business continuity, data security, information security, supplier requirements, etc.
- **Implementation of Risk Management in the Use of Information Technology by Nonbank Financial Services Institutions**: On March 9, 2021, the Indonesian Financial Services Authority issued this regulation, which requires non bank financial institutions to implement risk management in IT technology, involving requirements in multiple IT fields, such as information security, business continuity, data security, domestic transaction processing, supplier management, etc.

1.3 Definition

- **HUAWEI CLOUD**

  HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.

- **Customer**

  Refers to registered users who have entered into commercial relations with HUAWEI CLOUD

- **Service provider**

  An entity, including its branches providing services to a FI under an

  Outsourcing arrangement.

- **Cloud computing**

  Cloud computing refers to a type of internet-based computing that provides shared computer processing resources and data on demand according to the National Institute of Standards and Technology (NIST).

- **Disaster recovery plan**

  The interruption or damage caused by nature or human beings cannot be avoided in the business activities of financial institutions, such as earthquake, fire, flood, power failure, technical failure, human negligence, etc. The interruption or damage not only affects the technical capacity of financial institutions, but also affects the business operation of banks, especially the service to customers. Therefore, financial institutions must establish disaster recovery plans to ensure that business can continue to operate in the event of interruption or disaster, so as to protect the interests of stakeholders, with the focus on data recovery plans, key application systems and the operation of IT infrastructure.

  internal auditing

  An effective internal control system is an important part of the management of financial institutions. It can help the management of financial institutions

to protect assets, ensure reliable financial and management reports, and reduce the risks of losses, violations and breaches of prudence. As a part of the internal control system, IT internal audit needs to evaluate the implementation of IT independently and objectively to improve the efficiency and effect of risk management, internal control and good governance, including the audit of data center, disaster recovery, applications, etc.

2 HUAWEI CLOUD Security and Privacy Compliance

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of international and industry **security compliance certifications** ensuring the security and compliance of businesses deployed by cloud service customers.

HUAWEI CLOUD services and platforms have obtained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers(CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.

Certification	Description
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.

Certification	Description
CSA STAR Gold Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD Fusion Sphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.

Certification	Description
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.

Regional standard certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.

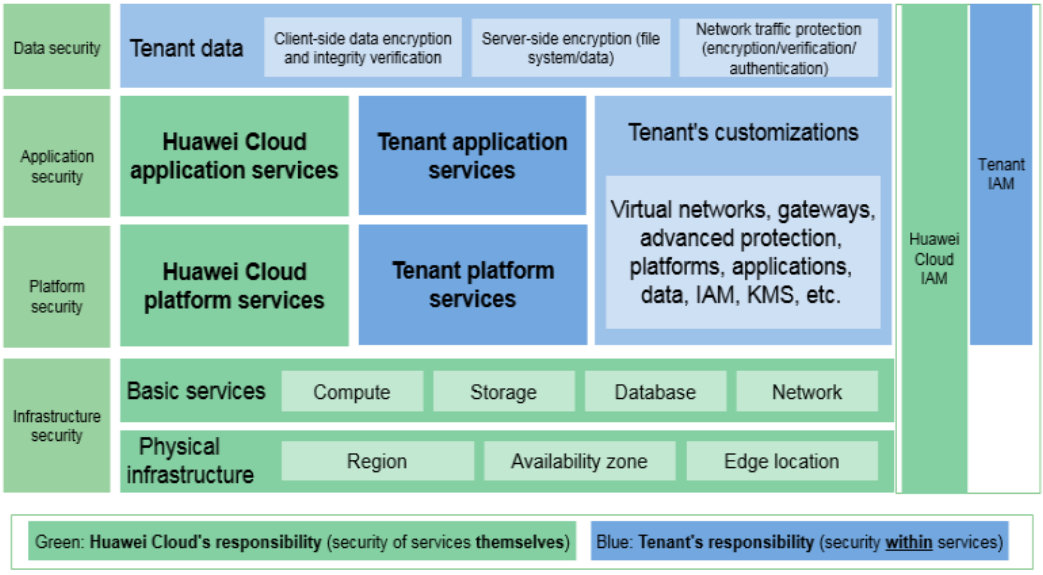
Certification	Description
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) (China)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certification.
TRUCS (China)	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification Cyberspace Administration of China (CAC) (China)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.

Certification	Description
OSPAR Certification (Singapore)	OSPAR is an audit report issued by the Association of Banks in Singapore (ABS) to outsourcing service providers. HUAWEI CLOUD passed the guidelines (ABS Guidelines) of the Association of Banks of Singapore (ABS) on controlling the objectives and processes of outsourcing service providers, proving that HUAWEI CLOUD is an outsourcing service provider that complies with the control measures Certification the ABS Guidelines.
TISAX (Europe)	TISAX (Trusted Information Security Assessment Exchange) is a security standard for information security assessment and data exchange in the automotive industry launched by the Verband der Automobilindustrie (VDA) and the European Automobile Industry Security Data Exchange Association (ENX). The passing of the TISAX indicates that HUAWEI CLOUD has met the European-recognized information security standards for the automotive industry.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance Certification please refer to the official website of HUAWEI CLOUD "**Trust Center - Compliance**"

3 HUAWEI CLOUD Security Responsibility Sharing Model

Due to the complex cloud service business model, cloud security is not the sole responsibility of one single party, but requires the joint efforts of both the customer and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help customers to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the customer and HUAWEI CLOUD:



As shown in the above model, the privacy protection responsibilities are distributed between HUAWEI CLOUD and customers as below:

HUAWEI CLOUD: The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application,

and data layers, in addition to the identity and access management (IAM) cross layer function.

Customer: The primary responsibilities of the customers are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a customer subscribes on HUAWEI CLOUD, including its customization of HUAWEI CLOUD services according to its needs as well as the O&M of any platform, application, and IAM services that the customer deploys on HUAWEI CLOUD. At the same time, the customer is also responsible for the customization of the security settings at the virtual network layer, the platform layer, the application layer, the data layer, and the cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the effective management of its users and identities.

For details on the security responsibilities of both Customers and HUAWEI CLOUD, please refer to the **HUAWEI CLOUD Security White Paper** released by HUAWEI CLOUD.

4 HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD "**Worldwide Infrastructure**".

5 How HUAWEI CLOUD Meets and Assists Customers to Meet No. 38_POJK.03_2016 Regulations on Risk Management in Commercial Banks Using Information Technology and its amendments

On December 14, 2016, the Indonesian Financial Services Authority issued the regulations of No.38_POJK.03_2016, which puts forward requirements for IT risk management of financial institutions in many aspects, such as business continuity, data security, information security, supplier management, etc.

Based on the requirements for information technology utilization efficiency and risk management, the Indonesian Financial Services Authority issued the Amendment on June 18, 2020, which revised the provisions of POJK MRT on data centers and disaster recovery centers.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

5.1 Risk management of information technology implementation

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 8	(1) Banks must implement effective risk management in the use of Information Technology. (2) Implementation of risk management as mentioned in paragraph (1) must at least include: a. active supervision by the board of Commissioners and Directors; b. sufficient policies and procedures on the use of Information Technology; c. sufficient processes of identification, measurement, monitoring and risk control on the use of Information Technology; d.	Customers shall establish methods and procedures for cyber security risk management in line with their organizational strategies	HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment. HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts an annual risk assessment and increases the number of risk assessments for major changes in information systems, a significant change in the company's business, or a significant change in laws, regulations or standards. It also carries out strict security management for outsourcers, and regularly audits and evaluates its suppliers. HUAWEI CLOUD develops and maintains an internal risk management framework to identify, analyze and manage risks that have been identified. A formal risk assessment is performed at least annually to determine the likelihood and impact of identified risks. Procedure is established to guide the Management for risk calculation and risk classification which determine the likelihood and impact of identified risks. The likelihood and impact associated with each risks is determined independently,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	internal control systems for the use of Information Technology; (3) Implementation of risk management must become an integral part during every stage of Information Technology use, from the process of planning, construction, development, operation, maintenance, up to the discontinuation and the disposal of Information Technology resources.		considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by Management. Additionally, at least monthly, HUAWEI CLOUD organizes meetings to discuss the assessment on the risks which have been identified in relation to network security and privacy protection. Corresponding follow-up actions are taken and documented to ensure the risks have been managed appropriately based on Huawei's risk management requirements.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 11	In the process of developing and acquiring information technology, banks must implement controls to generate confidential and integrated systems and data to support the achievement of bank objectives, including: Establish and implement consistent procedures and methodologies for information technology development and procurement; b. Implement project management in system development; c. Adequate testing during the development and procurement of systems, including joint testing with user work, to ensure the accuracy and consistency of systems and user requirements, as well as the	Customers should ensure that business processes and business applications are properly managed in network security risk management.	Project management framework Huawei Cloud has developed a complete project management method and implemented practices based on CCM5/CMMI, ISO 9001:2000 and PMI frameworks, enabling qualified project management professionals to successfully implement projects around the world. System development life cycle and design security Huawei Cloud pursues a new DevOps process, has the ability to rapidly and continuously iterate, and integrates Huawei's security development lifecycle (SDL). In addition, a highly automated new security lifecycle management method and process, called DevSecOps, has been gradually formed to ensure the smooth and flexible implementation of DevSecOps together with cloud security engineering capabilities and tool chains. Huawei Cloud manages the development environment hierarchically, and implements physical isolation, logical isolation, access control, data transmission channel approval, audit and other protection measures. To meet customer compliance requirements, Huawei Cloud strictly complies with the security coding specifications issued by Huawei. In addition, we also introduced the daily inspection of static code scanning tools, and the generated data will be input into the cloud service continuous integration/ continuous deployment (CI/CD) tool chain for control and cloud service product quality assessment by using quality thresholds. The source code shall be reviewed and approved by the change manager before compilation. Developers cannot

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	compatibility of one system with another; d. Development and maintenance of appropriate documentation systems; e. Conduct application change management; (f) Ensure that the Bank's information technology systems display information in its entirety;		approve and compile code. Before any cloud product or cloud service is released, the static code scanning alarm must be cleared to effectively reduce the problems related to code extension. All cloud services have passed multiple security tests before release. The test environment is isolated from the production environment to avoid using production data or sensitive production data for testing, and needs to be cleared after use.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 15	(1) The bank must set up a disaster recovery plan. (2) The bank must ensure that the disaster recovery plan described in paragraph (1) can be effectively implemented, so that the bank's business continuity can continue to operate in the event of disaster and/or interruption of the information technology facilities used by the bank. (3) According to the results of business impact analysis, banks are obliged to conduct at least one test of disaster recovery plan for all important applications and infrastructure within one year, and let information technology users participate in it. (4) The bank is obliged to review the	The customer shall formulate network security policies and procedures, obtain the approval of the person in charge or representative of the organization, and distribute them to relevant internal and external organizations of the organization	Huawei Cloud has rich business continuity management and disaster recovery strategies and processes. The business continuity plan is prepared and reviewed by the business continuity management team every year, and updated according to the review results. The business continuity management team performs business impact analysis and risk assessment every year, including determining key business processes, maximum tolerable downtime, recovery time objectives, minimum service levels, and the time required to restore services. The report identifies and records the threats that may cause the interruption of Huawei's cloud services and resources, and designs corresponding strategies for different service interruption scenarios of Huawei's cloud products. The results of business impact analysis and risk assessment are recorded in the risk assessment report. According to the plan, Huawei Cloud conducts business continuity drills and tests for all products within its scope at least annually. Record and review the results of business continuity drills and tests. According to the requirements of the internal business continuity management system, Huawei Cloud has formulated a sound recovery strategy to support the key businesses of the continuous operation of cloud services. Customers have disaster data backup centers in two places. In case of failure, the system will automatically transfer customer applications and data from the affected area to ensure business continuity on the premise of meeting compliance policies.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	disaster recovery plan at least once within one year.		Huawei Cloud has also deployed a global server load balancing center. Customer applications can be deployed in the data center. Even if one data center fails, it can balance the traffic load to other centers..

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 19	(1) The Bank must have internal audit guidelines for the use of Information Technology organized by the Bank itself and/or by Information Technology service providers. (4) Banks are required to submit to the Financial Services Authority: a. the results of the review as referred to in paragraph (3) accompanied by suggestions for improvement as part of the review report; and b. the results of the internal audit of Information Technology as part of the implementation report and the main points of the internal audit results, as stipulated in the provisions regarding the implementation of standards for	The Client shall be subject to an independent cyber security audit to determine compliance with recognized audit standards and cyber security frameworks. The network security audit of customers shall be conducted according to the internal audit manual and audit plan of the organization	Huawei's internal audit team reports directly to Huawei's Board of Directors and executive management. Stringent auditing activities play a key role in both promoting the adoption of cybersecurity processes and standards and assuring the delivery of results. Huawei has set up a dedicated security audit team to periodically review compliance with security laws and regulations worldwide as well as internal security requirements. The team dedicates over ten members to perform a two month long annual audit on HUAWEI CLOUD operations worldwide, paying close attention to such HUAWEI CLOUD aspects as legal, regulatory, and procedural compliance; business goal and milestone accomplishment; integrity of decision making information; and security O&M risks. Audit results are reported to Huawei's Board of Directors and executive management, who ensure that any and all identified issues are properly resolved and closed.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	the implementation of the internal audit function.		

5.2 Information technology implementation provided by banks or information technology service providers

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 20	(1) The Bank organizes Information Technology. (2) The implementation of Information Technology as referred to in paragraph (1) may be carried out by the Bank itself and/or Information Technology service providers. (3) In the event that the implementation of the Bank's Information Technology is carried out by an Information Technology service provider as referred to in paragraph (2), the Bank shall: f. monitor and evaluate the reliability of Information Technology service providers on a regular basis regarding	The contract signed between the customer and its service provider shall clearly list the service content and level provided, as well as the network security responsibilities and obligations of the service provider under the contract. Customers should only measure and evaluate the network security requirements of their outsourcing policies and processes on a regular basis. The network security audit of customers shall be conducted according to the internal audit manual and audit plan of their organization.	Huawei has established a dedicated safety audit team to review compliance with global safety laws and regulations and internal safety requirements. Huawei's internal audit team reports directly to the board of directors and senior managers of the company to ensure that the problems found are solved and ultimately closed. Strict audit activities play a key role in promoting the process and standards of network security and ensuring results are delivered. In addition, HUAWEI CLOUD has established a complete supplier selection and management mechanism, including day-to-day monitoring and supplier performance management, but also regularly conducts risk assessment for suppliers. HUAWEI CLOUD will inform FIs of problems identified in audits and reevaluate them within the organization, particularly if the problems have a significant impact on the business of the financial institution. HUAWEI CLOUD provides a unified communication interface with the outside world. It is responsible for collecting and handling complaints from customers and issuing announcements to financial customers from regulatory agencies. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	performance, reputation of service providers, and continuity of service provision; g. provide access to internal auditors, external auditors, and the Financial Services Authority to obtain data and information whenever needed; h. provide access to the Financial Services Authority to the Database in a timely manner, both for current data and for past data; and i. ensuring the Information Technology service provider: 1. have experts who have reliability supported by certificates of expertise academically and / or professionally in accordance		by customers. HUAWEI CLOUD has constructed a complete security system from security technology, security system, personnel management and other aspects in accordance with the most authoritative security standards in all regions of the world, and has obtained numerous security certifications at home and abroad. This allows users to enjoy a secure and trustworthy cloud platform and cloud services. Huawei advocates company-wide for a mindset and practice wherein "everyone understands security", cultivating a security culture that is present 24/7, as well as dynamic and competitive throughout the company. The impact of such a culture runs through talent recruitment, new-hire orientation, initial and ongoing training, internal transfer, and internal retraining, all the way up to employment termination.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	with the needs of organizing Information Technology; 2. implement Information Technology control principles adequately as evidenced by the results of an audit conducted by an independent party; 3. providing access to the Bank's internal auditors, external auditors appointed by the Bank, the Financial Services Authority, and/or other parties in accordance with regulatory provisions the laws and regulations are authorized to conduct examinations in order to obtain the necessary data and information in a timely manner whenever needed;		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	4. declare that it has no objection in the event that the Financial Services Authority and/or other parties who in accordance with the law are authorized to conduct an examination, will conduct an examination of the service provision activities provided; 5. as an affiliated party, maintain the security of all information including the Bank's secrets and customers' personal data; 6. can only carry out partial transfer of activities (subcontracting) based on the Bank's approval as evidenced by written documents; 7. report to the Bank any critical events that may result in significant financial losses		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	and/or disrupt the smooth operation of the Bank; 8. submit the results of Information Technology audits conducted by independent auditors periodically on the implementation of Data Centers, Disaster Recovery Centers, and/or Information Technology-Based Transaction Processing, to the Financial Services Authority through the Bank concerned; 9. provide a tested and adequate Disaster Recovery Plan; 10. willing to the possibility of terminating the agreement before the term of the agreement ends (early termination); and		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	11. fulfill the service level in accordance with the service level agreement between the Bank and the Information Technology service provider. (4) The use of Information Technology service providers by the Bank as referred to in paragraph (3) must be based on a written agreement which at least contains the willingness of the Information Technology service providers to organize and/or perform the matters as referred to in paragraph (3).		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 21	(1) The Bank is obliged to place the Electronic System at the Data Center and Disaster Recovery Center in the territory of Indonesia. (2) The Bank can only place the Electronic System at the Data Center and/or Disaster Recovery Center outside the territory of Indonesia as long as it obtains approval from the Financial Services Authority. (4) The approval of the Financial Services Authority as referred to in paragraph (2) may be granted in the event that the Bank: a. fulfill the requirements as referred to in Article 20 paragraph (3), paragraph (4), and paragraph (5);	Assurance customers need to develop disaster center plans, and the system should be deployed to continuously monitor data centers and disaster events nationwide. If the customer conducts a sexual review at the business system supplier, it is required to submit other materials such as risk analysis reports overseas and include legal options in the supplier's authorized service, and approve it together with the supplier's authorized service.	HUAWEI CLOUD has been launched in many countries or regions around the world. HUAWEI CLOUD's infrastructure adopts a model of deploying multiple geographic regions and multiple availability zones around the world. HUAWEI CLOUD can flexibly replace computing instances and store data within multiple geographic regions or between multiple availability zones within the same region. Each zone is an independent fault maintenance domain, that is, each availability zone is physically isolated. Customers can choose the availability zone for system deployment according to their own needs. If the customer chooses to deploy the electronic system in an overseas availability zone, HUAWEI CLOUD can arrange for a special person to actively cooperate with the customer to provide relevant certificates to obtain approval from the Financial Services Authority. HUAWEI CLOUD provides the online "HUAWEI CLOUD User Agreement" and "HUAWEI CLOUD Service Level Agreement", which stipulate the service content and service level provided, as well as the responsibilities of HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed offline contract templates, which can be customized according to the needs of different customers. High Availability of Infrastructure ● HUAWEI CLOUD implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers"

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	b. submit the results of the country risk analysis; d. Ensure that information regarding the Bank's secrets is only disclosed to the extent that it complies with the laws and regulations in Indonesia as evidenced by a cooperation agreement between the Bank and the Information Technology service provider; e. ensure that written agreements with Information Technology service providers also contain a choice of law clause; f. submit a statement of no objection from the supervisory authority of the Information Technology service provider outside the		data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance, ensuring business continuity. HUAWEI CLOUD has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure. ● Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZ within the same region. Each AZ is an independent, physically isolated fault maintenance domain, has its own UPS and on-site backup power generator, and also connects to a power grid different than any other AZ. All AZs connect to multiple tier-1 telecom providers for redundancy, eliminating the risk of single point of failure. ● Users can and should take full advantage of all these regions and AZs in their planning for application deployment and

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	territory of Indonesia that the Financial Services Authority can conduct an examination of the Information Technology service provider; h. ensure that the benefits of the plan to place the Electronic System outside the territory of Indonesia for the Bank are greater than the burden borne by the Bank; and		operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). Compliance In regions within our cloud services coverage, HUAWEI CLOUD actively facilitates dialogues with local regulators in order to better understand their concerns and requirements, share HUAWEI CLOUD's knowledge and experience, and continue to bolster the legal and regulatory compliance posture of HUAWEI CLOUD's technologies, services, and security. Furthermore, HUAWEI CLOUD shares with our customers the reports of legal and regulatory compliance audits, avoiding non-compliance violations caused by inadequate information disclosure to our customers. HUAWEI CLOUD also ensures that our tenant contracts accurately specify the security responsibilities of both sides. HUAWEI CLOUD continues to foster and strengthen customers' trust in our services by obtaining cross-industry, crossregion cloud security certifications as well as other security certifications targeting key industries and regions, striving toward a secure cloud environment built for and trusted by regulators, customer executives, and tenants. Cloud's Security Responsibilities With regard to tenant data, HUAWEI CLOUD is responsible for providing comprehensive data

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			protection functions to achieve confidentiality, integrity, availability, durability, authentication, authorization, and non-repudiation while also being responsible for the security of related functions. However, HUAWEI CLOUD is merely the trustee of tenant data whereas a tenant retains sole ownership of its data and controls its data usage. HUAWEI CLOUD prohibits any O&M personnel from accessing tenant data without proper authorization. HUAWEI CLOUD pays close attention to changes in internal and industry security compliance requirements and is responsible for ensuring regulatory and industry compliance as required for HUAWEI CLOUD services. HUAWEI CLOUD shares our compliance practices with our tenants and conducts internal and independent evaluations on our compliance posture for security standards specific to the industries that HUAWEI CLOUD serves, with evaluation results kept reasonably transparent to our tenants.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 23	(1) Banks are required to organize Information Technology-Based Transaction Processing in the territory of Indonesia. (2) Information Technology Based Transaction Processing can be carried out by service providers in the territory of Indonesia.	The customer shall ensure that the data center is located in Indonesia, or when using cloud services overseas, it shall obtain the approval of the financial regulatory authority.	The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the customer is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our customers. We will also openly and transparently tackle cloud security challenges standing shoulder-to-shoulder with our customers and partners as well as relevant governments in order to meet all the security requirements of our cloud users. HUAWEI CLOUD has obtained many authoritative security and privacy protection certificates in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on HUAWEI CLOUD. For more details, please refer to **HUAWEI CLOUD Security White Paper**.

5.3 Reporting

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 31	(1) The Bank is required to report critical events, misuse, and/or crimes in the implementation of Information Technology that can and/or have resulted in significant financial losses and/or disrupted the smooth operation of the Bank. (2) The report as referred to in paragraph (1) must be submitted immediately to the Financial Services Authority via electronic mail or telephone followed by a written report no later than 7 (seven) working days after the critical event and/or abuse or crime is known.	The customer shall formulate network security incident management strategy, establish security incident reporting and decision-making process, and adopt appropriate response plan and communication strategy. When a network security incident occurs, the customer shall report the incident improvement suggestions to the Financial Services Authority or other relevant regulatory authorities according to the specified requirements.	HUAWEI CLOUD reviews and summarizes the impact and handling processes of security incidents, and informs and reports to the corresponding affected users and regulatory departments as required. HUAWEI CLOUD has developed a complete process for incident management and notification. If an incident occurs on the HUAWEI CLOUD Base Platform, relevant personnel will analyze the impact of the incident according to the process. If the incident has or will have an impact on the cloud service customers, HUAWEI CLOUD will start to notify customers of the incident. The contents of the notice include but are not limited to description of the incident, the cause, impact, measures taken by HUAWEI CLOUD, and measures recommended for customers. To assist customers in meeting the requirements of cybersecurity incidents reporting to CISO, HUAWEI CLOUD has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			and implement emergency plans and recovery processes to minimize the impact on services.

6 How HUAWEI CLOUD Meets and Assists Customers to Meet No.21/SEOJK.03/2017 Notice on Risk Management in Commercial Banks Using Information Technology

The regulations of No. 21/SEOJK. 03/2017 issued by the Indonesian Financial Services Authority put forward various requirements for IT risk management of financial institutions, including requirements in multiple IT fields, such as business continuity, data security, information security, supplier requirements, etc.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

6.1 MANAGEMENT

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
1.5Project Management	According to Article 11 of POJK MRTI, the Bank is obliged to take control measures to create a fully confidential and integrated system and data, and support the realization of the Bank's objectives, including the application of project management in system development	The customer shall establish a project management framework to ensure that the delivery and practice process of IT projects meet their project objectives and requirements. For each IT project plan, the customer should consider the project scope, activities, milestones, and deliverables for each phase.	Huawei Cloud has developed a complete project management method and implemented practices based on CCM5/CMMI, ISO 9001:2000 and PMI frameworks, enabling qualified project management professionals to successfully implement projects around the world.

6.2 DEVELOPMENT AND PROCUREMENT

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
2.2. Control Measures in Development and Procurement	In conducting IT development and procurement, the Bank is required to take control measures to produce systems and data that are confidentiality and integration which maintained and support the achievement of the Bank's objectives as stipulated in Article 11 POJK MRTI. In addition to the control measures as set out in Article 11 POJK MRTI, control measures may also include: a. Ensure the system is developed according to user needs; b. Ensure the compatibility of one system with another so that they can continue to function properly (interoperability and compatibility); c. own the source code of the software developed specifically for the Bank concerned (proprietary) so that the source code can be accessed if needed for the purposes of examination and investigation. d. adequately identifying, measuring and controlling the risks that may arise in	Customers should conduct due diligence before selecting service providers, especially in terms of governance, risk and compliance management mechanisms. The Client shall develop a list of reputable service providers and be able to determine whether there are any viable alternative preferred service providers.	For the security of the development process, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	relation to IT development and procurement; e. Determine the risk appetite and risk exposure acceptable to the Bank in relation to IT development and procurement; f. have procedures for system development in emergencies; and g. Ensure the separation of the development and operational environments, including separating the human resources responsible for the development process from the human resources who carry out the Bank's operational activities.		automated new security life cycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD ensures the secure introduction and use of open source and third party software based on the principle of strict entry and wide use. HUAWEI CLOUD has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			HUAWEI CLOUD has pursued the new DevOps process, which features rapid and continuous iteration capabilities, and integrated the HUAWEI security development lifecycle (SDL). In addition, gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD hierarchically manages the development environment and implements protection measures such as physical isolation, logical isolation, access control, and data transmission channel approval and audit.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
2.3. Bank Development and Procurement Policies, Standards and Procedures must have policy, standards	IT development and procurement procedures as stipulated in Article 8 POJK MRTI. The IT development and procurement process must always be under the control of the IT work unit and managed by project management. Project management can take the form of a working team whose members at least come from the IT working unit and the IT user working unit, whose task is to ensure that the system has been developed with a good structure and has accommodated user needs. If procurement during process development process and changes, such as changes in user requirements or changes in supporting technology, change management procedures must be designed, implemented and properly documented. Development and procurement policies, standards and procedures must consider the following: a. IT development stages include at least: 1) identification and analysis of user needs;	The customer shall establish a framework to manage its system development life cycle (SDLC) as required. The customer shall determine, define and record the functional requirements of the IT system, covering system performance, flexibility and security control.	For the security of the development process, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security life cycle management methodology

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	2) defining user requirements; 3) system design; 4) programming; 5) Testing; 6) Implementation; 7) post-implementation review; 8) maintenance; and 9) disposal. b. The IT procurement process includes: 1) procurement standards; 2) procurement project guidelines; 3) escrow agreement; 4) software purchase, licensing and maintenance contracts; 5) Maintenance; 6) warranty; 7) dispute resolution; 8) change of agreement; 9) security; and 10) subcontracting to other parties. c. Policies, standards, and procedures that the Bank needs to have in place for project management and change management.		and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD ensures the secure introduction and use of open source and third party software based on the principle of strict entry and wide use. HUAWEI CLOUD has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. HUAWEI CLOUD has pursued the new DevOps process, which features rapid

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			and continuous iteration capabilities, and integrated the HUAWEI security development lifecycle (SDL). In addition, gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD hierarchically manages the development environment and implements protection measures such as physical isolation, logical isolation, access control, and data transmission channel approval and audit.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
2.4. Development and Procurement Risk Management Process	2.4.1. Risk Measurement related to Development and Procurement Measurement level risk at process development IT development and procurement process depends on related factors, among others: a. conformity with business strategic plans and applicable regulations; b. changes to the scope of the system or process; c. separation of development, test and operational environments, including access arrangements for developers, testers and users; d. application system plan to be obtained through purchasing a package without modification, purchasing a package with modification, developing internally or by a third party; e. the scope and criticality of the system or the number of business units affected; f. complexity of the processing type of the application to be developed (batch, real-time, client or server, parallel distributed); g. volume and transaction value of the	The customer shall establish a change management procedure to identify, classify and prioritize changes according to the importance of information assets. The customer shall regularly review and update the safety requirements of change management and the effectiveness of the process according to the planned frequency. The customer shall regularly review and update the safety requirements of change management and the effectiveness of the process according to the planned frequency.	HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment. HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts an annual risk assessment and increases the number of risk assessments for major changes in information systems, a significant change in the company's

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	application system to be developed; h. classification and data sensitivity of the system to be developed; i. impact on the data (read, download, upload, update, or alter); j. the level of experience and capability of the vendor, if the system is purchased or developed by a third party; k. adequacy of the number and capabilities of personnel included in the development team; l. compatibility of the selected platform and application with the Bank's architecture; m. dependency of the developed system with the existing system; n. mismatch of the number of users with the initial development plan or changes in the organizational structure during the development process; o. changes to provisions; p. the existence of new risks or risks that may arise from technologies under development or the risk of technological obsolescence; q. audit weaknesses or weaknesses encountered in		business, or a significant change in laws, regulations or standards. It also carries out strict security management for outsourcers, and regularly audits and evaluates its suppliers. HUAWEI CLOUD develops and maintains an internal risk management framework to identify, analyze and manage risks that have been identified. A formal risk assessment is performed at least annually to determine the likelihood and impact of identified risks. Procedure is established to guide the Management for risk calculation and risk classification which determine the likelihood and impact of identified risks. The likelihood and impact associated with each risks is determined independently, considering each risk category.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	self-assessment; and r. mismatch of development implementation with target completion time. 2.4.2. Risk Control in Development and Procurement At every stage of IT development and procurement, the Bank must mitigate the risks that have been identified and measured by several control means that have been established in the policy, standards, and procedures of the Bank's IT development and procurement. After mitigation, the Bank must monitor the controlled risk and residual risk because any disruption that may affect the IT development and procurement plan and process, may ultimately impact the Bank's operational activities. 2.4.2.1. Risk Control at Development In order to control risks related to IT development, the Bank must be able to ensure that the system development carried out is in accordance with policies, standards and procedures for each stage of development. This is done by paying attention to:		Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by Management. Additionally, at least monthly, HUAWEI CLOUD organizes meetings to discuss the assessment on the risks which have been identified in relation to network security and privacy protection. Corresponding follow-up actions are taken and documented to ensure the risks have been managed appropriately based on Huawei’s risk management requirements.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	a. The system development plan is in line with user needs and the Bank's business policy direction; b. The system design developed included user requirements at the initiation and planning stages and complied with application control standards involving the participation of internal audit. Based on its purpose, control is divided into controls that are preventive, detection or findings, or correction. Controls that must be carried out include at least: 1) Input Control This includes at least checking the validity or correctness of the data, data range, parameters, and duplication of inputted data; 2) Process Control Ensure processes work accurately and can store or reject information. Process controls that can be automated by the system include at least error reporting, transaction logs, sequence checking, and file backups; and 3) Output Control Ensure the system manages information securely and distributes processed information		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	appropriately and deletes information that has passed the retention period; c. programming deliverables are built based on design specifications with a documented test plan to make it easier to track changes to the application system; d. conducting a series of tests by defining the scope of the test scenario, assessing the results of the test, making improvements to the system until the test report is approved; e. implementation of the new system can run with the old system with the preparation of installation, file migration, data conversion, technical guidance documents, and training; and f. The results of the implementation of the system run well on an ongoing basis with regular reviews of the results of maintenance effectiveness. 2.4.2.2. Risk Control at Procurement In order to control risks in procurement, the Bank must establish vendor selection criteria and review the vendor's capabilities, among others, related to financial conditions,		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	support levels, and security controls, before making a choice of products or services from the vendor. The Bank should review the licensing agreement to ensure that the rights and responsibilities of each party are clear and reasonable. The Bank's legal counsel should confirm that performance guarantees, access to source code, copyright, and security of the software or data, are clearly set out before management signs the agreement. Matters that need to be considered are: a. ensure that the procurement process is in accordance with the Bank's policies, standards and procedures as well as applicable provisions related to procurement; and b. to enter into all agreements that have sufficient legal force.		

6.3 IT OPERATIONAL ACTIVITIES

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.2. Policies, Standards and Procedures related to IT Operational Activities	In accordance with Article 12 POJK MRTI, the Bank is required to ensure the continuity and stability of IT operations and mitigate risks that could potentially disrupt the Bank's operational activities. The Bank must have policies that cover every aspect of IT operations and are tailored to the complexity of the Bank's IT operations. IT operational aspects include Data Center, capacity planning and monitoring, hardware and software configuration management, and Database management. Procedures contain responsibilities, accountabilities, authorizations, and guidelines for operational activities. In addition, management must establish hardware and software standards used in the operational, testing, and development environments in the Bank's IT operations.	Customers should establish and regularly review formal information security policies and processes. Customers establish network security capabilities and control management requirements based on business requirements. The customer shall consider the security principles in the design when formulating and applying network security control requirements.	According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. In addition, HUAWEI CLOUD focuses on the development of security awareness among employees and outsourcing personnel, and has developed an applicable security awareness training program that is applied regularly.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.3 IT Operational Activity Risk Management Process	Risk management of IT operational activities must consider: a. Events or activities that can disrupt operations include: 1) technology investment errors including improper implementation, vendor failure, improper definition of business requirements, incompatibility with existing systems, or software obsolescence, including loss of vendor support for hardware and software used by the Bank; 2) System development and implementation issues include inadequate project management, cost and time overruns, programming errors, failure to integrate or migrate from existing systems, or failure of a system to meet user needs; 4) system failures including network, interface, hardware, software, or internal communication failures; and 5) breaches in system security including external and internal security breaches, programming fraud, or computer viruses. b. The level of IT operational risk that	The Client shall define and implement infrastructure security standards. The customer shall regularly review and update the control of application network security according to the planned frequency.	To complement our customers' compliance requirements, Huawei's dual role as a developer and cloud service operator of cloud technology is responsible for its CSP infrastructure and the security of its own services (i.e. IaaS, PaaS and SaaS). HUAWEI CLOUD ensures that development, configuration, deployment, and operation of various cloud technologies is secure. Therefore, in the initial phase, HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. In addition, in order to ensure the safe and stable

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	depends on related factors, among others: 4) The acquisition of applications may be through the purchase of packages without modification, purchase of packages with modification, and/or development in-house or by third parties; 11) adequacy of the number and capability of implementing staff;		operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness.

6.4 COMMUNICATION NETWORK

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.2 Policies, Standards, and Procedures related to Communication Network	In accordance with Article 13 POJK MRTI, Banks are required to provide communication networks that meet the principles of confidentiality, integrity, and availability. To fulfill this obligation, the Bank must have policies, standards, and procedures as guidelines in providing communication networks to ensure that the operational continuity and security of communication networks are maintained. Communication network policy is the direction and purpose of communication network management that will be organized by the Bank, for example related to the application of encryption on communication networks. Communication network standards are a number of parameters set by the Bank to fulfill the communication network policy, for	The customer shall formulate network security policies and procedures, obtain the approval of the person in charge or representative of the organization, and distribute them to the internal and external relevant organizations of the organization. The customer shall establish a formal system and network security architecture to ensure that the organization's network is free from security risks. The customer shall regularly track and monitor the implementation of the network security risk disposal plan.	According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. In addition, HUAWEI CLOUD focuses on the development of security awareness

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	example, the use of Secure Socket Layer (SSL) on the communication network session layer. The communication network procedure is a series of technical steps to be taken by the Bank to fulfill the communication network standard. Policies, standards and procedures that need to be established include at least: a. network performance and capacity planning; b. securing communication networks (network access control, including remote access); c. change management (setup, configuration, and testing); d. network management, network logging, and network monitoring; e. use of the internet, intranet, e-mail, and wireless (including mechanisms for using		among employees and outsourcing personnel, and has developed an applicable security awareness training program that is applied regularly.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	communication networks); f. problem handling procedures; g. backup and recovery facilities; and h. agreements and SLAs that are in accordance with the Bank's needs and are monitored regularly if the communication network used by the Bank is organized by an IT service provider.		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.3 Communication Network Risk Management Process	4.3.1. Risk Control a. The use of communication network technology provides various conveniences and benefits for the Bank and customers, however, it is necessary to pay attention to the risks that may arise, among others: 1) loss of data/ information; 2) loss of data/ information integrity; 3) incomplete data/ information being transmitted; 4) loss of confidentiality of information; 5) unavailability of communication networks due to disruption or disaster; and 6) loss/damage of communication network devices. b. In controlling risks on communication networks, the Bank must pay attention to the following matters: 1) Communication Network Design The communication network must be	The customer shall establish a formal system and network security architecture to ensure that the organization's network is free from security risks. The customer shall regularly track and monitor the implementation of the network security risk disposal plan.	HUAWEI CLOUD has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering IT governance/ management, information system development and acquisition, IT operation, communication network, information security and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. HUAWEI CLOUD has built a comprehensive information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files, and the key directions and objectives of information security,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	designed in such a way that it is efficient but also dynamic to anticipate future developments. At this stage, there are several things that need to be considered, namely: a) determination of communication network topology; b) planning capacity (capacity planning) communication network; c) selection of communication network media; d) hardware backups, alternative routing, or alternative providers; e) physical security and logic: i. placement of network devices in locations that are safe from natural disturbances and access by unauthorized persons; and ii. setting system parameters of network devices. f) The availability of an audit trail, at least for changes to parameter settings and access rights of communication		including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. In addition, the system performs real-time evaluation of the security posture of

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	network devices as well as the use of those access rights. 2) Access Control Access control on the communication network is very important and must be considered because the communication network is the main door to enter the Bank's information system. If not managed properly, information security is jeopardized. In implementing access control, there are several things that must be considered by the Bank, namely: a) Access to communication networks by users is based on business needs with attention to information security aspects; b) Segmenting the communication network based on both physical and logical segments, such as the separation between development and operational environments; c) If physical separation cannot be done, the Bank must logically		HUAWEI CLOUD, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping HUAWEI CLOUD take necessary security precautions. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability information, including the cloud, is immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	separate the communication network and monitor security access on the network communication; d) decisions to connect to communication networks outside the Bank must be in accordance with security requirements and formally approved by management prior to implementation; e) implement controls that can limit unauthorized or unexpected network traffic; f) the configuration of communication network devices should be well organized. Unnecessary functions or services should be disabled; g) use of communication network security devices, such as firewalls, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS); h) the use of additional communication network monitoring devices (network		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	management system) with due regard to security; and i) Periodic testing of communication network security, for example by penetration testing. 4.3.2. Risk Monitoring Monitoring of risks that may arise in the communication network used by the Bank includes, among others: a. The available audit trail should be monitored regularly to detect any irregularities early; b. Communication network performance is measured periodically based on availability and response time; c. Banks should monitor the capacity utilized and required for the business development plan compared to the installed capacity; d. The Bank should monitor and follow up on intrusions or attacks on communication networks; and e. The Bank must periodically review		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	the granting of access to users to ensure that the access granted is still in accordance with the duties and authorities. In addition, it is necessary to review the communication network users in the Bank that has access to communication networks outside the Bank.		

6.5 INFORMATION SECURITY

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2 Policies, Standards and Procedures related to Information Security	In accordance with Article 16 POJK MRTI, the Bank must ensure that information security is implemented effectively by paying attention to at least: a. Information security is intended to ensure that the information managed is maintained confidentiality, integrity, and availability effectively and efficiently by taking into account compliance with the provisions; b. Information security is carried out on aspects of technology, human resources, and processes in the use of IT; c. information security implemented based on the results of a risk assessment of the information held by the Bank; and d. availability of incident handling management in information security.	The customer shall formulate network security policies and procedures, obtain the approval of the person in charge or representative of the organization, and distribute them to the internal and external relevant organizations of the organization. The network security policies and procedures established by customers can refer to the technical security standards in the industry.	According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. In addition, HUAWEI CLOUD focuses on

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			the development of security awareness among employees and outsourcing personnel, and has developed an applicable security awareness training program that is applied regularly.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2.3.2 Human Resource Management Procedures	HR management procedures include at least: d. agreements with Bank employees, consultants, honorary employees, and employees of IT service providers must include IT security provisions that are in line with the Bank's information security policy. For example, it is necessary to have a clause stating that they must maintain the confidentiality of the information they obtain in accordance with the classification of the information; e. In addition to the agreement between the Bank and the IT service provider company, all employees of the IT service provider company assigned to the Bank must sign a non-disclosure statement, including the confidentiality of information for the purpose of protecting customer data; f. Training and/or socialization on information security must be provided to	The Client shall formulate and implement the network security requirements for employees before, during and after employment. The customer shall regularly monitor and evaluate the effectiveness of personnel network security management requirements and processes according to the planned frequency. The customer shall include in the labor contract and confidentiality clauses the requirements and responsibilities of network security that the personnel shall abide by. The customer shall regularly conduct network security awareness training for in-service employees. The client shall ensure that the relevant authority and assets of the employee are reviewed and recovered after	According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. In addition, HUAWEI CLOUD focuses on the development of security awareness among employees and outsourcing

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	Bank employees, consultants, temporary employees, and employees of IT service providers. This training and/or socialization is provided in accordance with the roles and responsibilities of employees and IT service providers; g. The Bank must establish sanctions for violations committed by HR against information security policies; and h. The Bank should establish procedures governing the return of assets and the change or termination of access rights of Bank employees, consultants, temporary employees, and employees of IT service providers due to changes in duties or completion of employment or agreements.	the employee leaves the company.	personnel, and has developed an applicable security awareness training program that is applied regularly.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2.3.3 Physical and Environmental Security Procedures	Physical and environmental security procedures include at least: a. Critical information processing facilities (e.g. mainframes, servers, computers and active network devices) should be provided with adequate physical and environmental safeguards to prevent unauthorized access, damage and other interference; b. Physical and environmental security of critical information processing facilities includes, among others, room dividers, access control (e.g. use of access control cards, Personal Identification Number (PIN), and biometrics), completeness of security equipment in the room, such as alarms, fire detectors and extinguishers, air temperature and humidity meters, and CCTV cameras, as well as maintenance of room and equipment cleanliness, such as from dust,	When the customer uses the service, the physical and environmental responsibility is borne by the cloud service cloud security.	Data center site selection: When choosing a location for a HUAWEI CLOUD data center, HUAWEI CLOUD factors in the risks of potential natural disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a HUAWEI CLOUD data center. For example, HUAWEI CLOUD data centers are always located in areas where there are no potentially hazard-causing laboratories, chemical plants, or other hazardous zones within 400 meters. Site selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water, and telecommunication circuits. Physical access control: HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	cigarettes, food, drinks, and flammable items; c. Supporting facilities such as air conditioning, electrical resources, and fire alarms must be ensured for their capacity and availability in supporting the operations of information processing facilities; d. assets belonging to IT service providers such as servers and switching tools must be clearly identified and given adequate protection, for example by implementing adequate security, dual control or placing them separately from the Bank's assets; and e. periodic maintenance and inspection of information processing facilities and supporting facilities in accordance with established procedures.		24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. Security guards strictly review and regularly audit user access privileges. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system (WMS). Designated

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis to ensure that unauthorized personnel have no access to data centers. Safety measures: HUAWEI CLOUD data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. Security guards routinely patrol data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			trigger sound and light alarms. Electrical safety: HUAWEI CLOUD data centers employ a multi-level safety assurance solution to ensure 24/7 service availability and continuity. Daily electricity consumption at data centers relies on dual power supply from different power substations. Data centers are equipped with diesel generators, which are run in the event of power outage, and also Uninterruptible Power Supply (UPS), which provides temporary power as a backup. Data center power lines have voltage regulator and overvoltage protection. Power supply equipment is configured with redundancy and power lines run in parallel to ensure power supply to data center computer systems. Temperature and humidity control: HUAWEI CLOUD data centers are fitted with high precision air conditioning and automatic adjustment of centralized

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			humidifiers to ensure that computer systems operate optimally within their specified ranges of temperature and humidity. Hot and cold air channels for computer cabinets are properly designed and positioned. Cold air channels are sealed to prevent isolated hot spots. The space beneath the raised floor is used as a static pressure box to supply air to computer cabinets. Fire control: The computer room complies with Indonesia's "Technical Requirements for Fire Protection Systems in Buildings and Environments (26/PRT/M/2008)", and also complies with the requirements of the National Fire Protection Association. Fire-retardant and fire-resistant cables are used, which are laid in pipes or trunkings, and a leakage detection device is installed. An automatic alarm and automatic fire extinguishing system is deployed, which can quickly and accurately detect and

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			report the fire situation. The automatic alarm system is linked with the power supply, monitoring and ventilation equipment. Even if there is no one on duty due to unexpected situations, the automatic fire extinguishing system can be turned on to control the fire. Routine monitoring: HUAWEI CLOUD personnel conduct daily patrols and routine inspections of power, temperature, humidity, and fire controls in all data centers, which allows for the timely discovery of safety hazards and ensures smooth operation of all data center equipment. Water supply and drainage: The water supply and drainage system at each HUAWEI CLOUD data center is designed, implemented, and operated to an exacting standard, ensuring that main valves function as per specification and key personnel are aware of valve locations. This prevents water damage to the data center equipment,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			especially computer information systems. Data center buildings reside on elevated ground with peripheral green drains and each floor is raised, which speeds up water drainage and reduces the risk of flooding. Data center buildings all meet Level-1 water resistance requirements, ensuring that rainwater does not seep through roofs and walls into the data center, and that there is proper drainage in case of a flood. Anti-static control: HUAWEI CLOUD data centers are paved with anti-static flooring materials and have wires connect raised floor brackets to grounding networks, discharging static electricity from computer equipment. Data center roofs are fitted with lightning belts, and power lines are fitted with multiple level lighting arresters, diverting the current safely to grounding networks.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2.3.4 Access Control Procedures	Access control procedures include at least: a. Physical and logical access control; b. Banks must apply identification and authentication methods according to the risk analysis. The authentication method used can be one or a combination of "what you know" (including PIN and password), "what you have" (including cellphone, magnetic card with chip, and token), "something you are" (including biometric such as retina and fingerprint); c. The Bank must have a formal written procedure approved by management on user administration that covers user registration, change and deletion, both for internal users and external users, such as vendors or IT service providers; d. granting access refers to the principle based on business needs and with the minimum possible access; e. The Bank must establish control	The customer shall establish an identity authentication and access control management mechanism to restrict and supervise the access to the system. The customer shall ensure that all internal and external account types are included in the account management requirements. The customer shall implement role-based access control and authority management, in accordance with the principle of minimum awareness and use as needed.	Customers can manage user accounts using cloud resources through **HUAWEI CLOUD Identity and Access Management (IAM)**, including support for password authentication, IAM also supports multi factor authentication as an option. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. In addition, **Huawei's Cloud Trace Service (CTS)** provides collection, storage, and querying of operational records for a variety of cloud resources to support

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	procedures through provision of initial password or PIN to users by taking into account, among others: 1) The initial password or PIN must be changed during the first login; 2) passwords or PINs are given securely, for example through double-layered carbon paper so that they are only known by authorized parties; 3) The initial password or PIN is unique for each user and not easily guessed; 4) the owner of the user-id, especially from Bank employees, honorary employees, and employees of IT service providers, must sign a statement of responsibility or agreement on the use of the user-id and password or PIN when receiving the initial user-id and password or PIN; and 5) The default password or PIN of the operating system, application system, database		common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	management system, and network and security devices must be changed by the Bank before implementation and the default user-id of the system must be changed.		same business to ensure that personnel with different responsibilities in different positions are limited to access the equipment under their role. To meet customer compliance requirements, administrators of HUAWEI CLOUD-related systems must first pass two factor authentication before they can access the management plane through a springboard. All operations are logged and sent to the centralized log audit system in time. The audit system has a strong data retention and query capability to ensure that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD also has a dedicated internal audit department which will regularly audit the activities of the O&M process. Additionally, HUAWEI CLOUD only has remote access to its internal systems through the HUAWEI CLOUD unified management access gateway and SVN

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			authority. Moreover, strong log auditing is supported on the access gateway to ensure that the operation and maintenance personnel can locate their actions on the target host.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2.3.5 IT Operational Security Procedures	IT operational security procedures include at least: f. The Bank must conduct periodic reviews of IT operational services performed by IT service providers. The review period must be stipulated in the cooperation agreement between the Bank and the IT service provider; and	The customer shall implement the protection of malicious code/ software and viruses. The customer shall follow the established network security incident management strategy, continuously monitor and analyze the security logs of each system, and timely detect and respond to security events and incidents. The Client shall define and implement infrastructure security standards.	In order to ensure the safe and stable operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness. HUAWEI CLOUD will arrange for someone to actively cooperate with the audit. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			audited by third parties every year. Additionally, HUAWEI CLOUD has developed a complete supplier management mechanism that regularly assesses the performance of suppliers (including outsourcing personnel). The results of the assessment are used as an important reference for the next procurement. HUAWEI CLOUD also has security compliance and confidentiality agreements with suppliers, including outsourced individuals.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
5.2.3.6. Information Security Monitoring Procedure	The Bank must conduct monitoring in order to detect efforts that threaten information security with methods determined based on risk or the level of criticality of the Bank's information or IT assets. Monitoring can be done in real time to provide alerts when there are activities that are classified as suspicious, for example brute force against administrator passwords or attempts to access servers on unreasonable ports, or carried out periodically, for example at the end of the day, based on the level of risk.	The customer shall formulate network security incident management strategy, establish security incident reporting and decision-making process, and adopt appropriate response plan and communication strategy. The customer shall follow the established network security incident management strategy, continuously monitor and analyze the security logs of each system, and timely detect and respond to security events and incidents.	HUAWEI CLOUD, as a CSP, is responsible for the management of infrastructure and major events of various cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has a centralized and complete log audit system. The large data security analysis system is used to correlate alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks, and predict attacks that have not yet occurred. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. HUAWEI CLOUD helps customers build a network security protection system to secure their cloud services. Customers at the Internet border

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			can detect and clean abnormal traffic and traffic attacks by doing the following: deploying Anti-DDoS services; partitioning and isolating key network partitions through **Virtual Private Cloud (VPC)** and deployment of a **Web Application Firewall (WAF)** to deal with web attacks to protect web application services and systems deployed in the DMZ area that are oriented to the external network. In order to ensure that the tenant business does not affect the management operation and that the equipment, resources and traffic will not be separated from effective supervision, HUAWEI CLOUD divides the communication plane of its network into a tenant data plane, business control plane, platform operation and maintenance plane, BMC (Baseboard Management Controller) management plane, and number based on different business functions, different security risk levels, and different

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			permissions to ensure that the network traffic related to different services is reasonably and safely diverted so as to facilitate the separation of responsibilities.

6.6 DISASTER RECOVERY PLAN

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
6.2 Policies, Standards and Procedures related to Disaster Recovery Plans	6.2.2. Procedures related to Disaster Recovery Plan c. Disaster Recovery Center The Bank must ensure the availability of a Disaster Recovery Center as a backup of the Data Center that can be operated if the Data Center cannot operate due to disruptions and/or disasters. In accordance with the alternative strategy chosen by the Bank, the Disaster Recovery Center can be managed by itself or by an IT service provider. In organizing the Disaster Recovery Center, the Bank must pay attention to the following matters: 1) The Disaster Recovery Center should be located at a location separate from the Data Center location, taking into account geographical factors: a) the geographic extent of a disturbance or disaster and its impact on the city or region where the Disaster Recovery Center is located; and	The customer should ensure that the security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space.	Customers can rely on HUAWEI CLOUD data center cluster multi region (Region) and multi availability zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world, so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load balanced management center, where the customers' applications enable N +1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. HUAWEI CLOUD has various policies and

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	b) analysis of risks associated with the location of the Disaster Recovery Center (such as not being located in an earthquake, flood, or lightning prone area) and being connected to a communications and power infrastructure that is different from the Data Center, as well as other facilities needed to keep a system running; 2) the vulnerability of the selected Disaster Recovery Center location to the possibility of riots and unrest; 3) The Disaster Recovery Center must have electricity supply and telecommunication facilities that can guarantee the operation of the Disaster Recovery Center; 4) systems in the Disaster Recovery Center must be compatible with the systems used in the Data Center and must be adjusted if changes occur in the Data Center; 5) Disaster Recovery Center is a restricted area; and 6) travel time to ensure the recovery		procedures for business continuity management and disaster recovery. Business continuity plans are established and reviewed by the business continuity management team annually, and the plans are updated according to results of the review. The business continuity management team performs business impact analysis and risk assessment every year, including identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service level and time needed to resume service. Threats that may lead to disruptions to HUAWEI CLOUD's business and resources are identified and documented in the reports, and corresponding strategies are designed for different service disruption scenarios of HUAWEI CLOUD's products. Results of the business impact analysis and risk assessment are documented in the risk evaluation report. HUAWEI

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	process at the Disaster Recovery Center.		CLOUD conducts a business continuity drill test at least annually in accordance with the plan for all in-scoped products. The results of the business continuity drill test are documented and reviewed. Simultaneously, HUAWEI CLOUD has developed its own business continuity plan, in addition to providing features such as improved infrastructure availability, redundant data backup, and disaster preparedness in available areas. The program focuses on major disasters such as earthquakes or public health crises to keep cloud services running and secure the customer business and data. Huawei will notify in advance if customer participation is required during the disaster testing of HUAWEI CLOUD. HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of GB

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			50174 Code for Design of Electronic Information System Room and T3+ standard of TIA-942 Telecommunications Infrastructure Standard for Data Centers. -The HUAWEI CLOUD O&M team regularly carries out risk assessments on global data centers to ensure that data centers strictly implement access control, security measures, routine monitoring and audit, emergency response and other measures. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers.

6.7 USE OF IT SERVICE PROVIDERS

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
9.4. Internal Control and Internal Audit	9.4.1. Monitoring and Supervision of IT Service Providers In the event that the Bank's IT implementation is carried out by an IT service provider, the Bank must still have an IT work unit and the highest official who leads the IT work unit. The bank should have a monitoring program to ensure that the IT service provider has performed the work or provided the services in accordance with the agreement. Resources to support this program may vary depending on the criticality and complexity of the systems, processes, and services that the IT service provider is working on. The Bank must conduct reviews before and after the employment of IT service providers to ensure that the Bank's risk management policies, standards and procedures have	The contract signed between the customer and its service provider shall clearly list the service content and level provided, as well as the network security responsibilities and obligations of the service provider under the contract. Customers should only measure and evaluate the network security requirements of their outsourcing policies and processes on a regular basis. The network security audit of customers shall be conducted according to the internal audit manual and audit plan of their organization.	HUAWEI CLOUD cooperates with customers to exercise supervision over cloud service providers. The online **HUAWEI CLOUD Customer Agreement** defines cloud service customers and Huawei's security responsibilities, and the **HUAWEI CLOUD Service Level Agreement** stipulates the service level provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed a negotiable offline contract template to address specific customer needs. For more information, please refer to **HUAWEI CLOUD Customer Agreement**. HUAWEI CLOUD will arrange for someone to actively cooperate with the audit. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	been carried out effectively. Furthermore, performance reviews and SLA achievements are conducted periodically and documented in the form of reports. Monitoring should be done on the IT service provider's audit report. 9.4.2. Internal Audit The Bank conducts audits of IT service providers on a regular basis, either conducted by the Bank's internal audit or external audit parties appointed by the Bank. The scope of the audit is in accordance with the scope of services as stated in the agreement. The audited areas include: a. IT systems; b. data security; c. internal control framework; and d. Disaster Recovery Plan. The Bank must ensure that the Financial Services Authority or other parties assigned by the Financial Services Authority have the right of		ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. Additionally, HUAWEI CLOUD has developed a complete supplier management mechanism that regularly assesses the performance of suppliers (including outsourcing personnel). The results of the assessment are used as an important reference for the next procurement. HUAWEI CLOUD also has security compliance and confidentiality agreements with suppliers, including outsourced individuals. HUAWEI CLOUD will provide audit samples to verify the effectiveness of HUAWEI CLOUD security and compliance control measures, such as security system management documents, operating records and system logs. This is in accordance with the requirements of external audit

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	access to IT service providers to obtain records and transaction documents, as well as Bank information stored or processed by IT service providers as well as the right of access to reports and audit findings on IT service providers related to IT services.		institutions. If special circumstances lead to insufficient time to cover audit samples, HUAWEI CLOUD will cooperate with the audit institutions to indicate the reasons in the audit report. In view of all the problems found in the audit process, HUAWEI CLOUD will assess the potential impact of these problems on financial industry customers with the assistance of audit institutions and according to the risk assessment mechanism. If after evaluation, problems that may seriously affect the availability, integrity and confidentiality of customer business/ data are identified, HUAWEI CLOUD will classify such problems as security incidents, and promptly notify the affected customer groups according to the established customer notification process. This includes the description of the problem, the impact of the problem, and the next remedial plan. At the same time, HUAWEI CLOUD will rectify the problem

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			according to the internal security incident management process, and the audit institutions will reassess the problem after the rectification is completed.

7 How HUAWEI CLOUD Meets and Assists Customers to Meet No.4_POJK.05_2021 Regulations on Risk Management in the Use of Information Technology by Non-Bank Financial Institutions

The No.4_POJK.05_2021 issued by the Indonesian Financial Services Authority stipulates the risk management requirements for the implementation of IT technology by non bank financial institutions (referred to as "LJKNB"), involving requirements in multiple IT fields, such as information security, business continuity, data security, domestic transaction processing, supplier management, etc.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

7.1 ADEQUACY OF THE PROCESS OF IDENTIFYING, MEASURING, CONTROLLING, AND MONITORING THE RISKS OF USING INFORMATION TECHNOLOGY

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 11	(1) LJKNB must have policies and procedures in carrying out the process of identification, measurement, control, and monitoring of the risk of using Information Technology as referred to in Article 3 paragraph (2) point c. (2) LJKNB must identify, measure, control, and monitoring of the risk of using Information Technology in accordance with the policies and procedures as referred to in paragraph (1). (3) The process of identifying, measuring, controlling, and monitoring the risks of using Information Technology as referred to in paragraph (2) shall be carried out at least on aspects related to Information	The customer shall regularly track and monitor the implementation of the network security risk disposal plan. The customer shall review and revise the design and effectiveness of the newly implemented network security control.	HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment. HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts an annual risk assessment and increases the number of risk assessments for major changes in information systems, a significant change in the company's business, or a significant change in laws, regulations or standards. It also carries out strict security management for outsourcers, and

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	Technology as referred to in Article 9 paragraph (3). (4) In the case of LJKNB using the Information Technology Service Provider, the LJKNB is obliged to ensure that the Information Technology Service Provider applies risk management as set out in the Financial Services Authority Rules.		regularly audits and evaluates its suppliers. HUAWEI CLOUD develops and maintains an internal risk management framework to identify, analyze and manage risks that have been identified. A formal risk assessment is performed at least annually to determine the likelihood and impact of identified risks. Procedure is established to guide the Management for risk calculation and risk classification which determine the likelihood and impact of identified risks. The likelihood and impact associated with each risks is determined independently, considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by Management. Additionally, at least monthly, HUAWEI CLOUD organizes meetings to discuss the assessment on the risks which have been identified in relation to network security and privacy protection. Corresponding follow-up actions are taken and documented to ensure the risks have been

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			managed appropriately based on Huawei's risk management requirements.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 12	(1) In developing Information Technology, LJKNB must take control measures to produce a system that supports: a. achievement of LJKNB objectives; and b. maintained confidentiality and data integration. (2) The control measures referred to in paragraph (1) include at least: a. establish and apply the methodology and procedures for the development and procurement of Information Technology consistently; b. implement project management in the development and procurement of systems; c. perform appropriate tests in the development and installation of a system, including tests with a user working unit, to ensure the safety and functioning of the system as required by the user and the compatibility of	The customer shall establish a change management procedure to identify, classify and prioritize changes according to the importance of information assets. The customer shall ensure the code security of externally developed applications. The customer shall establish a formal change approval mechanism, and the change can only be made after the authorization and approval of the business principal, the network security functional department and the change committee.	HUAWEI CLOUD has developed a complete project management approach and is CCM5/ CMMI, ISO 9001:2000 and PMI framework based practices which have enabled successful project implementations over the world by qualified project and project management professionals. To meet customer compliance requirements, HUAWEI CLOUD has also developed change management procedures to application and infrastructure changes. After the change application is generated, the change manager shall make a change level judgment and submit it to the HUAWEI CLOUD change committee, which shall pass the review before implementing the change as planned. All changes are fully validated prior to application through class production, bad condition testing, gray release, Blue Green Deployment, etc. to ensure that the change committee has a clear understanding of the change action, duration, fallback action of the change failure, and all possible impacts. HUAWEI CLOUD isolates development, testing,

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	the system with the other system; d. documentation on the development, installation and maintenance of the Information Technology system; e. have information technology system change management; f. ensure that the LJKNB Information Technology system is able to display information as a whole; and g. ensuring that a written agreement is made with the software in the event that the software affects the continuity of the LJKNB's operations and was created by another party.		and production environments, and strictly controls the flow of unsensitized data into the testing environment; HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding. HUAWEI CLOUD provides online version of **HUAWEI CLOUD Service Level Agreement,** which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence by FIs. Customers' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 16	(1) LJKNB must have a Disaster Recovery Plan. (2) LJKNB must ensure that the Disaster Recovery Plan as referred to in paragraph (1) can be implemented effectively so that the operational continuity of the LJKNB continues to run during disasters and/or disruptions to the Information Technology facilities used by LJKNB. (3) LJKNB must conduct trials of the Disaster Recovery Plan as referred to in paragraph (1) on all core applications and critical infrastructure in accordance with the results of periodic impact analysis by involving work units of Information Technology users. (4) LJKNB must review the Disaster Recovery Plan as referred to in paragraph (1) periodically. (5) LJKNB shall determine the trial	The customer should ensure that the security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space.	HUAWEI CLOUD has various policies and procedures for business continuity management and disaster recovery. Business continuity plans are established and reviewed by the business continuity management team annually, and the plans are updated according to results of the review. The business continuity management team performs business impact analysis and risk assessment every year, including identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service level and time needed to resume service. Threats that may lead to disruptions to HUAWEI CLOUD's business and resources are identified and documented in the reports, and corresponding strategies are designed for different service disruption scenarios of HUAWEI CLOUD's products. Results of the business impact analysis and risk assessment are documented in the risk evaluation report. HUAWEI CLOUD conducts a business continuity drill test at least annually in accordance with the plan for all in-scoped products. The results of the business continuity

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	period as referred to in paragraph (3) and review as referred to in paragraph (4) of the policy in writing.		drill test are documented and reviewed.

7.2 SYSTEM OF INTERNAL CONTROL OVER THE USE OF INFORMATION TECHNOLOGY

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 20	(1) LJKNB must have internal audit guidelines for the use of Information Technology held by LJKNB itself and/or by the Information Technology service provider. (2) LJKNB must review the internal audit function in the use of Information Technology periodically. (3) LJKNB must set the review period as referred to in paragraph (2) of the policy in writing.	The network security audit of customers shall be conducted according to the internal audit manual and audit plan of their organization.	Huawei has established a dedicated safety audit team to review compliance with global safety laws and regulations and internal safety requirements. Huawei's internal audit team reports directly to the board of directors and senior managers of the company to ensure that the problems found are solved and ultimately closed. Strict audit activities play a key role in promoting the process and standards of network security and ensuring results are delivered. In addition, HUAWEI CLOUD has established a complete supplier selection and management mechanism, including day-to-day monitoring and supplier performance management, but also regularly conducts risk assessment for suppliers. HUAWEI CLOUD will inform FIs of problems identified in audits and reevaluate them within the organization, particularly if the problems have a significant impact on the business of the financial institution. HUAWEI CLOUD provides a unified communication interface with the outside world. It is responsible for collecting and handling complaints from customers and issuing announcements to financial customers from regulatory agencies.

7.3 IMPLEMENTATION OF INFORMATION TECHNOLOGY BY LJKNB AND / OR INFORMATION TECHNOLOGY SERVICE PROVIDERS

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 21	(1) The implementation of Information Technology by LJKNB can be carried out independently and/or using the Information Technology service provider. (2) In the event that the implementation of LJKNB Information Technology is carried out by the Information Technology service provider as referred to in paragraph (1), LJKNB must: a. responsible for the implementation of risk management; b. have a work unit organizing Information Technology; c. supervise the implementation of LJKNB activities organized by information technology service providers; d. select Information	The contract signed between the customer and its service provider shall clearly list the service content and level provided, as well as the network security responsibilities and obligations of the service provider under the contract. The customer shall regularly evaluate the compliance with the contract and supplier management procedures, as well as the performance of the service contract by the supplier. The customer shall regularly evaluate the effectiveness of the network security control of the contract and supplier management procedures. The customer shall require the participation of the network security function in formulating the contract and	HUAWEI CLOUD will arrange for someone to actively cooperate with the audit. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. Additionally, HUAWEI CLOUD has developed a complete supplier management mechanism that regularly assesses the performance of suppliers (including outsourcing personnel). The results of the assessment are used as an important reference for the next procurement. HUAWEI CLOUD also has security compliance and confidentiality agreements with suppliers, including outsourced individuals. Huawei has established a dedicated safety audit team to review compliance with global safety laws and regulations and internal

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	Technology Service Providers based on cost-benefit analysis by involving the Information Technology Maintenance Unit; e. monitor and evaluate the performance, reputation of the service provider and the adequacy of the provision of information technology services; f. provide access to internal auditors, external auditors, internal auditors of the LJKNB group, and/or the Financial Services Authority to obtain data and information whenever necessary; g. provide access to the Financial Services Authority to the Database in a timely manner, both for the latest data and for past data; and h. ensure the Information Technology Service Provider: 1. possess expertise with the support of an academic and/or professional certificate of competence in	supplier management process, consider the applicable network security baseline requirements, and conduct regular network security audits and reviews. The customer shall specify the network security requirements for withdrawal, termination or renewal in the contract signed with the supplier. The customer shall specify the mutual confidentiality agreement in the contract signed with the supplier.	safety requirements. Huawei's internal audit team reports directly to the board of directors and senior managers of the company to ensure that the problems found are solved and ultimately closed. Strict audit activities play a key role in promoting the process and standards of network security and ensuring results are delivered. In addition, HUAWEI CLOUD has established a complete supplier selection and management mechanism, including day-to-day monitoring and supplier performance management, but also regularly conducts risk assessment for suppliers. HUAWEI CLOUD will inform FIs of problems identified in audits and reevaluate them within the organization, particularly if the problems have a significant impact on the business of the financial institution. HUAWEI CLOUD provides a unified communication interface with the outside world. It is responsible for collecting and handling complaints from customers and issuing announcements to financial customers from regulatory agencies.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	accordance with the retention of Information Technology; 2. implement the principles of the management of Information Technology in a manner consistent with the independent audit results; 4. declare no objection in respect of the Financial Services Authority and/or any other party in accordance with the rules of the statute empowered to carry out the inspection, shall carry out an inspection of the activities of the Information Technology Service provided; 5. to maintain the security of all information, including LJKNB secrets and consumer personal data, as a therapeutic party; 6. may carry out only part of the activities (subcontracts) in accordance with the consent of the LJKNB as demonstrated by		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	the written document; 7. report to the LJKNB any critical event which may result in significant financial losses and/or disturb the operational collapse of the LJKNB; 8. provide a tested and adequate Disaster Recovery Plan; 9. be willing to the possibility of termination of the agreement before the term of the agreement expires; 10. meet the service level in accordance with the service level agreement between LJKNB and the Information Technology service provider; and 11. have clear and measurable standard operating procedures in the implementation of its business. (3) The use of the Information Technology service provider as referred to in paragraph (2) by the LJKNB must be based on a written agreement containing at least		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	the willingness of the Information Technology service provider to comply with the provisions as referred to in paragraph (2) point h.		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 22	(1) LJKNB which has total assets up to IDR 500,000,000,000.00 (five hundred billion rupiah) required perform a backup of processed activity data using Information Technology, which is carried out periodically. (2) LJKNB which has total assets of more than IDR 500,000,000,000.00 (five hundred billion rupiah) up to IDR 1,000,000,000,000.00 (one trillion rupiah) must: a. own a Data Center; and b. perform backups of activity data processed using Information Technology, which is carried out periodically. (3) LJKNB must determine the period for re-recording activity data processed using Information Technology as referred to in paragraphs (1) and (2) of the policy in writing. (4) LJKNB: a. who has total assets of more than	The customer should ensure that the security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space. The customer shall formulate the security management strategy for backup and recovery, and define the organization's requirements for information, software and system backup	Customers can rely on HUAWEI CLOUD's data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	IDR 1,000,000,000,000.00 (one trillion rupiah); and/or b. the majority of which is carried out using Information Technology, must have a Data. (5)The Authority requests the LJKNB: fulfilling the criteria referred to in verse (1) for the possession of a Data Centre; and fulfilling the criterion of having a disaster recovery centre,		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 23	a statement letter of no objection from the supervisory authority of Information Technology service providers outside the territory of Indonesia that the Financial Services Authority is granted access to conduct inspections of Information Technology service providers;	The customer should ensure that the security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space. The customer shall ensure that representatives of key areas of financial institutions regularly identify the regulatory requirements related to network security, and optimize the network security policy within the organization according to the update of network security regulatory requirements or standards.	Customers can rely on HUAWEI CLOUD's data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 24	LJKNB is required to ensure that the Data Center and/or Disaster Recovery Center as referred to in Article 23 can guarantee the continuity of the LJKNB's business.	Financial institutions should establish their own business continuity mechanisms and develop RTO and RPO indicators to ensure their key businesses.	Customers can rely on HUAWEI CLOUD's data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. HUAWEI CLOUD has various policies and procedures for business continuity management and disaster recovery. Business continuity plans are established and reviewed by the business continuity management team annually, and the plans are updated according to results of the review. The business

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			continuity management team performs business impact analysis and risk assessment every year, including identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service level and time needed to resume service. Threats that may lead to disruptions to HUAWEI CLOUD's business and resources are identified and documented in the reports, and corresponding strategies are designed for different service disruption scenarios of HUAWEI CLOUD's products. Results of the business impact analysis and risk assessment are documented in the risk evaluation report. HUAWEI CLOUD conducts a business continuity drill test at least annually in accordance with the plan for all in-scoped products. The results of the business continuity drill test are documented and reviewed.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 25	(1) LJKNB are required to carry out Information Technology-Based Transaction Processing in the territory of Indonesia. (2) Information Technology-Based Transaction Processing may be carried out by service providers in the territory of Indonesia. (3) The implementation of Information Technology-Based Transaction Processing by the service provider as referred to in paragraph (2) may be carried out as long as: a. comply with the precautionary principle; b. meet the requirements as referred to in Article 21 paragraph (2) to paragraph (4); and c. pay attention to aspects of consumer protection.	The customer shall ensure that the data center is located in Indonesia, or when using cloud services overseas, it shall obtain the approval of the financial regulatory authority.	The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the customer is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our customers. We will also openly and transparently tackle cloud security challenges standing shoulder-to-shoulder with our customers and partners as well as relevant governments in order to meet all the security

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			requirements of our cloud users. HUAWEI CLOUD has obtained many authoritative security and privacy protection certificates in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on HUAWEI CLOUD. For more details, please refer to **HUAWEI CLOUD Security White Paper.**

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 26	(1) LJKNB is required to include plans for the use of Information Technology service providers in the operation of Data Centers, Disaster Recovery Centers, and/or Information Technology-Based Transaction Processing in the plans for developing LJKNB Information Technology. (2) The realization of the plan for the operation of a Data Center, Disaster Recovery Center, and/or Information Technology-Based Processing by the Information Technology service provider must be reported as part of the report on the realization of the business plan. (3) The obligations as referred to in paragraph (2) only apply to LJKNB that are required to submit a business plan realization report to the Financial Services Authority.	Financial institutions should establish their own business continuity mechanisms and develop RTO and RPO indicators to ensure their key businesses. The customer should ensure that the security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space.	HUAWEI CLOUD will arrange for someone to actively cooperate with the audit. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. Additionally, HUAWEI CLOUD has developed a complete supplier management mechanism that regularly assesses the performance of suppliers (including outsourcing personnel). The results of the assessment are used as an important reference for the next procurement. HUAWEI CLOUD also has security compliance and confidentiality agreements with suppliers, including outsourced individuals.

7.4 CONFIDENTIAL SECURITY OF CONSUMER PERSONAL DATA

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 30	In implementing Information Technology, LJKN are required to guarantee: a. the acquisition, processing, use, storage, updating, and/or disclosure of consumer's personal data is carried out based on the consent of the consumer concerned, unless otherwise stipulated by the provisions of laws and regulations; and b. the use or disclosure of consumer personal data in accordance with the purposes submitted to consumers at the time of data acquisition.	Customers should correctly and comprehensively identify personal data in the cloud, formulate policies that can protect the security and privacy of personal data, and select appropriate privacy protection measures to ensure the security of personal data, private data or confidential data.	After obtaining a customer's consent, HUAWEI CLOUD collects the customer's personal data that is necessary for the provision of services and sends a privacy notice to inform the customer of the types of personal data to be collected, collection purposes, processing means, time limit, etc. For example, HUAWEI CLOUD provides a Privacy Statement and the mechanism for customers to give and withdraw consent on its official website. When personal data is to be collected in offline marketing activities, a privacy notice is provided at a prominent position, and a consent option is provided. HUAWEI CLOUD also provides various configuration options on its official website. Customers can set the types of messages to be received and the means for receiving messages based on their preferences. For cloud services that involve personal data processing, HUAWEI CLOUD informs customers of the types of personal data to be processed and the means of processing and storage in the product documentation. Customers can take privacy protection measures accordingly.

7.5 REPORTING

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
Article 31	(1) LJKNB are required to report critical incidents, misuse, and/or crimes in the operation of Information Technology that may and/or have resulted in significant financial losses and/or disrupt the smooth operation of the LJKNB. (2) The report as referred to in paragraph (1) must be submitted to the Financial Services Authority no later than 5 (five) working days after the critical event and/or misuse or crime is known using the format as stated in the Appendix which is an integral part of this Financial Services Authority Regulation.	When a network security incident occurs, the customer shall report the incident improvement suggestions to the Financial Services Authority or other relevant regulatory authorities according to the specified requirements.	HUAWEI CLOUD has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. HUAWEI CLOUD has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			recommended for customers. In addition, HUAWEI CLOUD analyzes the root causes of security incidents and formulates preventive and preventive measures. HUAWEI CLOUD periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring. HUAWEI CLOUD has established a crisis communication plan to promptly disclose related incidents and notify customers in accordance, and implement emergency plans and recovery processes to minimize the impact on services in the event of an emergency that affects customer service continuity.

8 Conclusion

This article describes how HUAWEI CLOUD provides customers with cloud services that comply with the regulatory requirements of the financial industry in Indonesia. It also shows that HUAWEI CLOUD complies with key regulatory requirements issued by the Indonesian Financial Services Authority, which helps customers understand HUAWEI CLOUD's compliance with the regulatory requirements of the financial industry in Indonesia in detail, so that customers can safely and confidently store and process customer content data through HUAWEI CLOUD services. At the same time, to some extent, this paper also guides customers on how to design, build and deploy a secure cloud environment that complies with the regulatory requirements of the Indonesian financial industry on HUAWEI CLOUD, and helps customers better share the corresponding security responsibilities with HUAWEI CLOUD.

This white paper is for general reference only, and does not have any legal effect or constitute any form of legal advice. Customers should evaluate their own use of cloud services at their discretion, and be responsible for ensuring compliance with relevant Indonesian financial industry regulatory requirements when using HUAWEI CLOUD.

9 Version History

Date	Version	Description
October 2022	1.0	First release

