



Tencent Cloud User Guide to Financial Industry Regulations & Guidelines in Indonesia

April 2026

Copyright Notice

©2013-2026 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's prior written consent.

Trademark Notice

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parents, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is provided for reference purposes only. Tencent Cloud makes no express or implied warranties regarding the information contained herein. The content is provided “as is” and may be subject to change without prior notice, including URLs and references to external websites. You assume all risks associated with the use of this document.

This document does not grant any legal rights to intellectual property of Tencent products. You may copy and use the content internally for reference purposes only.

Examples described herein are for illustrative purposes and are fictitious. They should not be interpreted as indicating any actual association or relationship.

CONTENTS

01	Overview	
02	Tencent Cloud Security and Privacy Compliance	
	2.1 Global Compliance	4
	2.2 ISO/IEC Certification	4
	2.3 Regional and Industry Compliance.....	6
03	Tencent Cloud Security Responsibility Sharing Model	
04	Tencent Cloud Global Infrastructure	
05	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Risk Management in the use of Information Technology by Commercial Banks	
	5.1 Information Technology Management.....	17
	5.2 Information Technology Development and Procurement	21
	5.3 Information Technology Operation Activities	27
	5.4 Information Technology Communication Network..	48
	5.5 Information Security	54
	5.6 Disaster Recovery Plan	71
	5.7 Internal Audit	78
	5.8 Engagement of Information Technology Service Providers	79
	5.9 Reporting.....	88
06	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Implementation of Information Technology by Commercial Banks and Non-Bank Financial Institutions	
07	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of the Regulation of the Cyber Resilience and Security for Commercial Banks	
	7.1 Quality Assessment for Cybersecurity Risk Implementation	127
	7.2 Quality Assessment for Cybersecurity Resilience Implementation	136
08	Conclusion	
09	Version History	

01

Overview

The Financial Services Authority of Indonesia (Otoritas Jasa Keuangan, hereinafter referred to as "OJK"), as the regulatory body for Indonesia's financial services industry, its core responsibilities lie in ensuring that the country's financial system always adheres to the operating principles of transparency, safety, and efficiency through establishing and improving regulatory frameworks and strengthening industry supervision and management, thereby maintaining financial market order and public trust. With the in-depth advancement of global digital transformation, various financial institutions in Indonesia have continuously increased the application of electronic systems, optimizing business processes and improving operational efficiency and service quality by introducing digital tools. Against this backdrop, to prevent potential risks that financial institutions may encounter in the application of information technology and ensure the steady progress of financial digital transformation, OJK has successively formulated and issued a number of targeted policy documents, which clarify the risk management requirements for financial institutions in the use of information technology, providing clear regulatory guidelines and manuals for financial institutions to standardize their digital business operations and strengthen risk prevention and control.

Tencent Cloud closely monitors OJK's regulatory developments and official publications and is committed to supporting Indonesian financial institutions in meeting these regulatory requirements. This document explains how Tencent Cloud assists customers in complying with the following regulatory guidelines and circulars that customers focus on:

- [No 38/POJK.03/2016 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank](#)
- [POJK Regulation No 38/POJK.05/2020](#)
- [No 21/SEOJK.03/2017 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank](#)
- [No 11/POJK.03/2022 - The Implementation of Information Technology By Commercial Banks](#)
- [No 04/POJK.05/2021 - The Implementation of Risk Management in The Use of Information Technology by Non-Bank Institutions](#)
- [No.29/SEOJK.03/2022 - Cyber Resilience and Security for Commercial Banks\)](#)

02

Tencent Cloud Security and Privacy Compliance

Compliance is the foundation of Tencent Cloud's development. Tencent Cloud identifies and adopts advanced international and industry security standards, and complies with the requirements of different countries, regions, and industries. By continuously improving its internal management system and enhancing its security management and control capabilities, Tencent Cloud is fully committed to building cloud services that customers can trust.

At the same time, Tencent Cloud also actively participates in the development and promotion of industry security standards, adhering to the principle of "Compliance as a Service" to build and operate a secure and reliable cloud ecosystem.

Tencent Cloud has obtained a wide range of security and privacy compliance certifications through independent third-party audits and assessments. These certifications demonstrate that the security management and privacy protection frameworks meet relevant certification standards and industry best practices. For more information on Tencent Cloud compliance, please refer to the [Tencent Cloud Compliance Center](#). To request any relevant compliance certificates or reports, please submit a request through the [Compliance Document Download](#) for download.

Examples of Tencent Cloud's internationally recognized certifications, as well as regional and industry accreditations, are as follows:

2.1 Global Compliance

CSA STAR Certification	The CSA STAR cloud security assessment is an international certification launched by the Cloud Security Alliance (CSA), a globally recognized non-profit organization. It extends the ISO/IEC 27001 Information Security Management System and incorporates the Cloud Control Matrix (CCM), visualizing cloud-specific security challenges and providing users with a clear overview of security architecture evaluation.
------------------------	---

Leveraging years of accumulated security practices, Tencent Cloud has obtained the CSA STAR Gold Certification, demonstrating that its security governance framework meets internationally recognized cloud security standards.

SOC Audit	System and Organization Controls (SOC) Reports are a series of internal control reports for service organizations issued by professional third-party accounting firms in accordance with the standards of the American Institute of Certified Public Accountants (AICPA). As independent audit reports, SOC Reports cover control points related to security, availability, and confidentiality of the Tencent Cloud platform.
-----------	--

Depending on the type of attestation service, SOC Reports can be provided to cloud users and their auditors, offering valuable information to help assess and address risks associated with the service organization.

2.2 ISO/IEC Certification

ISO/IEC 22301: 2019 Certification	ISO/IEC 22301:2019 is an international standard for Business Continuity Management (BCM), providing a comprehensive and universal methodology to help organizations identify and respond to potential disruptive events, ensure the continuity of critical operations, reduce risks, and protect against significant impacts.
-----------------------------------	---

Tencent Cloud has obtained ISO/IEC 22301:2019 certification, demonstrating that it has established formal business continuity management processes to ensure operational stability and resilience.

ISO/IEC 27001: 2022 Certification	ISO/IEC 27001:2022 Information Security Management System is recognized globally as one of the most authoritative, rigorous, and widely adopted certification standards in the field of information security. Achieving this certification signifies that an organization has established a scientific and effective information security management framework to align business strategy with security governance, ensuring that information security risks are properly controlled and addressed. Obtaining ISO/IEC 27001:2022 certification further demonstrates Tencent Cloud's commitment to security and confirms its capability to deliver secure and reliable cloud products and services.
ISO/IEC 20000-1: 2018 Certification	ISO/IEC 20000-1:2018 is an international standard for IT Service Management (ITSM). It defines a structured approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving IT service management systems. The standard helps organizations consistently identify and manage IT-related issues, strengthen communication with users, and build a standardized service framework that supports continuous improvement. Tencent Cloud has obtained ISO/IEC 20000-1:2018 certification, covering cloud computing services, hosting services, and disaster recovery services, demonstrating its commitment to delivering reliable and customer-focused IT service management.
ISO/IEC 9001: 2015 Certification	ISO 9001:2015 is a globally recognized and mature quality management system standard. It provides a comprehensive framework and guiding principles for managing the entire lifecycle of products and services, ensuring consistent and stable delivery quality. Tencent Cloud has obtained ISO 9001 certification, covering cloud computing services, hosting services, and disaster recovery services. By implementing a quality management system, Tencent Cloud effectively achieves its quality objectives and ensures the reliability and operational excellence of its cloud products and services.
ISO/IEC 27017: 2015 Certification	ISO/IEC 27017:2015 is an international standard that supplements ISO/IEC 27002:2013, providing practical guidelines for cloud service information security. It offers specific security controls and implementation guidance for both cloud service providers and customers, strengthening the management of threats and risks unique to cloud computing environments. Tencent Cloud has obtained ISO/IEC 27017:2015 certification, demonstrating its adherence to internationally recognized best practices and its commitment to building a comprehensive cloud security management system that enhances overall cloud security capabilities.
ISO/IEC 27018: 2014 Certification	ISO/IEC 27018:2014 is a globally recognized standard for the protection of personally identifiable information (PII) in public cloud environments. It provides a set of best practices for cloud service providers to safeguard user privacy and ensure the security of personal data in cloud computing. Tencent Cloud has obtained ISO/IEC 27018:2014 certification, signifying that its personal information management system complies with stringent international requirements for personal data protection, offering customers greater trust and assurance in cloud security.
ISO/IEC 29151: 2017 Certification	ISO/IEC 29151:2017 is an international standard that defines control objectives, controls, and implementation guidelines for processing personally identifiable information (PII) to address risks and privacy requirements identified through risk and impact assessments.

Tencent Cloud has obtained ISO/IEC 29151:2017 certification, demonstrating that it has developed an appropriate security control framework based on its PII objectives and business needs, providing a high level of privacy protection for user PII in the cloud.

ISO/IEC
27701: 2019
Certification

ISO/IEC 27701:2019 is an extension of ISO/IEC 27001 and ISO/IEC 27002, providing requirements and guidelines for establishing, implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). It represents a significant milestone in the ongoing management of privacy risks.

Tencent Cloud has obtained ISO/IEC 27701:2019 certification, demonstrating that user privacy protection is a core element of its services and confirming the standardization and reliability of privacy protection across Tencent Cloud products.

2.3 Regional and Industry Compliance

C5 [Germany]

The Cloud Computing Compliance Criteria Catalogue (C5) was developed by the German Federal Office for Information Security (BSI) to verify the information security compliance of cloud service providers through standardized audits and reporting. C5 is widely recognized as a high-level security standard in the cloud services industry.

Tencent Cloud has passed the German C5:2020 basic and additional audit criteria, demonstrating that its data protection and information security practices meet the stringent requirements set by the German government.

TISAX
[Germany]

TISAX (Trusted Information Security Assessment Exchange) is an information security assessment and data exchange standard jointly launched by the German Association of the Automotive Industry (VDA) and the European Network Exchange (ENX). It enables mutual recognition of information security assessments within the automotive industry and provides a unified evaluation and exchange mechanism.

Multiple Tencent Cloud Internet Data Centers (IDCs), including those located in Beijing and Shenzhen, have passed TISAX Level 3 assessments, ensuring that all services deployed in these regions meet TISAX requirements and maintain a robust information security management system.

MTCS Tier3
[Singapore]

The Multi-Tier Cloud Security (MTCS) Standard was developed under the guidance of the Infocomm Development Authority of Singapore (IDA) and its Information Technology Standards Committee (ITSC). As a widely adopted cloud security standard, MTCS helps cloud service providers address customer concerns regarding data security, confidentiality, and the impact of cloud services on business operations.

Tencent Cloud has obtained MTCS Level 3 certification, indicating that it has implemented robust risk management mechanisms to ensure data security, confidentiality, and verifiable operational transparency for its cloud customers.

OSPAR
[Singapore]

The Outsourced Service Provider's Audit Report (OSPAR) is the outsourcing compliance standard for the Singapore financial industry. Based on the Singapore Standards on Assurance Engagement (SSAE 3000), it verifies the design and operational effectiveness of controls in three areas: entity-level controls, general IT controls, and service controls.

Tencent Cloud has obtained OSPAR attestation for multiple products and services in the Singapore region, demonstrating that its security capabilities

	meet the stringent requirements for financial services in Singapore and Southeast Asia.
Data Protection Trustmark (DPTM) [Singapore]	The Data Protection Trustmark (DPTM) was developed by Singapore's Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA) to help organizations demonstrate responsible data protection practices. Tencent Cloud has obtained the DPTM certification, indicating that it adopts robust and accountable data protection measures for customers, business partners, and regulators, and is capable of safeguarding the personal data it collects.
Cyber Trust Mark (CTM) [Singapore]	The Cyber Trust Mark (CTM) is a national-level cybersecurity certification launched by the Cyber Security Agency (CSA) of Singapore. The CTM framework adopts a risk-based methodology, covering 22 sub-domains across 4 core areas: governance and risk management, cybersecurity operations, resilience, supply chain and personnel security, as well as continuous improvement and leading practices. Tencent Cloud has attained the highest level (Tier 5) of the Cyber Trustmark (CTM). This certification underscores Tencent Cloud's advanced capabilities in cybersecurity governance, risk management, and operational resilience, positioning it as a trusted cloud service provider for regulated and high-demand sectors across the Asia-Pacific region.
KISMS [Korea]	The Korean Information Security Management System (K-ISMS) certification is a government-backed standard designed to help organizations in Korea consistently and securely protect their information assets in accordance with applicable laws and regulations. Tencent Cloud has obtained K-ISMS certification, enabling customers in Korea to demonstrate compliance with local legal requirements for safeguarding critical digital information assets. This achievement also reflects Tencent Cloud's enhanced capabilities in information security and threat response, ensuring more effective mitigation of potential security risks.
IT compliance audit in Malaysian financial industry	Bank Negara Malaysia (BNM), the Securities Commission (SC), and other Malaysian financial regulatory authorities have issued regulations for the financial services industry to govern the application of information technology in banking, insurance, securities, and other financial services in Malaysia, ensuring the reliability, security, and stability of financial information systems. Tencent Cloud demonstrates compliance through independent third-party audits, proving that the cloud services provided to financial customers in Malaysia strictly adhere to the regulatory requirements of the Malaysian financial industry.
IT compliance audit in Hong Kong Special Administrative Region (HKSAR) financial industry	The Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), and Insurance Authority (HKIA) have issued key regulatory requirements to govern the use of information technology by financial, insurance, and securities institutions. Tencent Cloud has successfully undergone independent third-party audits, demonstrating that it is a trusted cloud service provider for the financial industry. By taking a proactive approach to fulfilling strict compliance obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure.
IT compliance audit in	Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange

Thailand financial industry	Commission (OSEC), the Office of Insurance Commission (OIC), and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's compliance with Thailand's stringent financial industry regulatory requirements and its commitment to providing high-quality, compliant cloud services to financial sector customers.
IT compliance audit in Indonesian financial industry	Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan, OJK), and other Indonesian financial regulatory authorities have issued regulations for the financial services industry. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits confirm that Tencent Cloud strictly complies with the regulatory requirements of Indonesia's financial industry when providing cloud services to financial customers.
Indonesia SNI 27001	SNI 27001 certification, a national standard for information security management systems (ISMS) regulated by Badan Standardisasi Nasional (BSN) and accredited by independent third-party auditors. The SNI 27001 framework adopts a risk-based approach, with core requirements covering key dimensions: Establishment and continuous operation of a formal ISMS, Comprehensive risk assessment and targeted control measures, Compliance with local information security regulations and 14 critical security domains and Regular internal audits, management reviews, and continuous improvement. Tencent Cloud has obtained Indonesia's SNI 27001 certification, Tencent Cloud has demonstrated excellence in protecting information asset confidentiality, integrity, and availability—extending to cloud-specific security scenarios. The certification reflects Tencent Cloud's mature security management system and its ability to address evolving cyber risks in the Indonesian market.
IT compliance audit in Philippines financial industry	Financial institutions in the Philippines are required to comply with regulations issued by the Bangko Sentral ng Pilipinas (BSP) and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's ability to comply with the stringent regulatory requirements of the Philippine financial industry and its commitment to providing high-quality, compliant cloud services to financial sector customers.
The Motion Picture Association of America (MPAA)	The Motion Picture Association of America (MPAA) has established a set of best practice standards for securely storing, processing, and transmitting protected media content. This implementation guidance is intended to help application and cloud service providers working with MPAA members understand the requirements for content security. The components of the MPAA Content Security Model reference relevant ISO standards (ISO 27001 and ISO 27002), recognized security standards (such as NIST, CSA, ISACA, and SANS), and industry best practices. Tencent Cloud has obtained certifications including ISO 27001, ISO 27017,

	ISO 27018, PCI DSS, and CSA STAR, and has conducted self-assessments to ensure that its content management processes comply with the MPAA Content Security Model.
HIPAA [US]	Health Insurance Portability and Accountability Act (HIPAA) is to promote the use of electronic health records to improve the efficiency and quality of the healthcare system through enhanced information sharing. HIPAA focuses on protecting the security (including availability, integrity, and confidentiality) and privacy of Protected Health Information (PHI) during creation, receipt, maintenance, and transmission by covered entities and their business associates. Entities subject to HIPAA are required to implement appropriate security measures when processing, maintaining, and storing PHI. Tencent Cloud conducts self-assessments to ensure its capability to protect personal information and the effectiveness of its control measures in compliance with HIPAA requirements.
SEC Rule 17a-4 [US]	Tencent Cloud Object Storage (COS) has been certified by an independent third-party assessment firm specializing in records management and information governance, based on the technical requirements of the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Commodity Futures Trading Commission (CFTC). This certification provides assurance for customers operating in highly regulated environments, such as the financial services industry, regarding the non-rewriteable, non-erasable preservation method and object lock feature of Tencent COS, demonstrating Tencent Cloud's commitment to delivering secure and industry-compliant cloud products.
The center for Financial Industry Information Systems (FISC) [Japan]	To enhance the security of financial institutions, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions provide effective guidance for Japanese banks and financial institutions in building secure information systems and ensuring their stable operation. Tencent Cloud has assessed its control measures against these guidelines to confirm that relevant measures meet the requirements of the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions.
BS10012:2017 [UK]	BS10012:2017 was published by the British Standards Institution to provide organizations with a compliance framework and good practices for privacy protection. It guides businesses in establishing and maintaining a Personal Information Management System (PIMS) to ensure adequate and appropriate controls for protecting personal information. The standard has been updated and revised to align with the General Data Protection Regulation (GDPR). Tencent Cloud has obtained BS10012:2017 certification, demonstrating that its personal information management system meets international standards and industry best practices, enabling customers to better comply with GDPR privacy protection requirements.
CISPE Code of Conduct [EU]	The CISPE Code of Conduct is a pan-European, sector-specific code for cloud infrastructure service providers under Article 40 of the EU General Data Protection Regulation (GDPR). It helps organizations across Europe accelerate the development of GDPR compliant cloud-based services for consumers, businesses, and institutions. Tencent Cloud has awarded "Candidate" mark of CISPE Code of Conduct, which means the cloud service provider has fulfilled the self-assessment against the CISPE Code of Conduct requirements.

NIST CSF Certification	NIST CSF is a framework that focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risk as part of an organization's risk management process. It helps organizations adjust and prioritize their cybersecurity activities based on business needs, risk tolerance, and resources, and improve security and resilience by applying the framework's risk management principles and guidelines. Tencent Cloud has obtained NIST CSF certification from an independent third-party organization, which affirms the capability of its cybersecurity defense system and demonstrates its ability to effectively identify, resist, respond to, and manage security risks, protecting cloud assets and data and enhancing confidence in security and stability.
PCI DSS Certification	The Payment Card Industry Data Security Standard (PCI DSS) is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC). To enhance the security of cardholder data, PCI DSS provides a globally unified benchmark for technical and operational requirements to protect account data. It applies to all entities involved in payment card processing, such as merchants, processors, acquiring institutions, issuing institutions, service providers, and other entities that store, process, or transmit cardholder data. Tencent Cloud has passed PCI DSS certification and obtained Grade 1 Service Provider qualification, demonstrating its capability to provide secure and reliable payment services and protect cardholder data.
GxP Compliance	In the healthcare industry, GxP refers to a set of regulations, guidelines, or industry best practices that govern compliance-related activities for medical products such as pharmaceuticals, medical devices, and medical software applications. Tencent Cloud has published a GxP compliance white paper to explain how its management processes and technical measures help customers meet the requirements of GxP computerized systems and ensure the confidentiality, integrity, and availability of business data hosted on Tencent Cloud.

03

Tencent Cloud Security Responsibility Sharing Model

At present, more customers have chosen cloud computing security as one of the primary considerations when selecting cloud computing service providers and the products and services they provide according to their own needs.

In keeping with the open and collaborative principles of cloud computing, Tencent Cloud continues to enhance its cloud computing security services capabilities and work with customers to build better and more comprehensive security systems for cloud services and data. It is precisely due to these cloud computing features that Tencent Cloud currently provides products and services under the three cloud computing architectures of IaaS, PaaS, and SaaS, and has established the following information security responsibility sharing model based on information assets and product functionalities. In this model, the light blue part is defined as the responsibility of Tencent Cloud, the light gray part is the responsibility of customers, and the light green part indicates that Tencent Cloud and customers will share the corresponding responsibilities.

	IaaS	PaaS	SaaS	
Customer Responsibilities	Cloud Customer Data Security	Cloud Customer Data Security	Cloud Customer Data Security	Shared Responsibilities
	Cloud Customer Accounts and Access Control Policies	Cloud Customer Accounts and Access Control Policies	Cloud Customer Accounts and Access Control Policies	
	Cloud Security Configuration Policies	Cloud Security Configuration Policies	Cloud Security Configuration Policies	
	Cloud Application Security	Cloud Application Security	Cloud Application Security	
	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	
Tencent Cloud Responsibilities	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	Tencent Cloud Responsibilities
	Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security	

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

Tencent Cloud explains the different security attributes in the above figure as follows:

- **Cloud Customer Data Security:** Security management of the customers' business data within the cloud computing environment, including data uploaded, stored, distributed, processed, and otherwise handled customer business data.
- **Cloud Customer Accounts and Access Control Policies:** Tencent Cloud account information registered by customers, and all authorized activities under this account, including account information, passwords, access control policies, identity verification, and other related information. **Cloud Security Configuration Policies:** Security products and security configuration policies based on different scenarios and aligned with business security requirements to ensure the proper development or use of cloud products (including security products).
- **Cloud Application Security:** Security management of business-related application systems within the cloud computing environment, including application design,

development, release, operation and maintenance, and ongoing monitoring.

- Cloud Virtualized Network and Host security: Host and network security management in a cloud computing environment, where the network level includes virtual network, load balancing, security gateway, VPN, leased line, etc.; host level includes the underlying management of cloud products such as cloud computing, cloud storage, cloud databases (such as virtualization control layer, database management system, and disk array network) and use management (such as virtual host, image, CDN, file system, etc.).
- Cloud Platform and Product Security & Compliance: Inherent security and regulatory compliance of the cloud platform and the cloud products/services provided within the cloud computing environment.
- Physical and infrastructure security: Data center management, physical facility management, and physical server and network device management in the cloud computing environment.

For more information about the responsibility sharing model, please refer to the [Tencent Cloud Security White Paper](#).

04

Tencent Cloud Global Infrastructure

Tencent Cloud has deployed multiple data centers worldwide, forming a large-scale infrastructure network that provides fast, stable, and reliable services to global customers. Tencent Cloud has opened more than 20 geographic regions and operates over 60 availability zones across Mainland China, Asia-Pacific, North America, and Europe, offering strong technical support to enterprises, helping them meet regulatory requirements in different regions, and addressing the financial industry's needs for data localization and global business expansion to ensure compliance, security, and efficiency in data processing.

- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically independent data center within the same region, with separate power and network resources. This design ensures isolation between zones to prevent fault propagation (except in cases of large-scale disasters or major power failures), enabling continuous online services. By deploying instances in independent zones, users can protect applications from single-location failures.

Tencent Cloud currently operates over 2,300 acceleration nodes in Mainland China, covering multiple carriers, and more than 900 acceleration nodes overseas across 70+ countries and regions. By distributing content to global acceleration nodes and leveraging a global scheduling system, users can access content from the nearest node, reducing latency. Tencent Cloud also enhances data isolation and security through independent sites and technologies such as data encryption, access control, and audit tracking, preventing data leakage and unauthorized access while strengthening regional isolation and compliance.

For more information about Tencent Cloud infrastructure, please refer to [Tencent Cloud Global Infrastructure](#).

05

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Risk Management in the use of Information Technology by Commercial Banks

The continuous innovation of information technology provides critical support for empowering banking services. By effectively leveraging information technology, commercial banks can significantly improve their internal operational efficiency and optimize the quality of customer-oriented services. However, the in-depth application of information technology in bank operations has also increased the risks faced by banks. The use of information technology requires attention to the dynamic changes of relevant regulatory rules, as well as the development of national and international standards. In 2016, Indonesia's Financial Services Authority (OJK) issued [No 38/POJK.03/2016 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank](#) to regulate and improve the risk management of commercial banks in the process of using information technology. Its provisions mainly focus on the implementation of information technology risk management, the information technology operations of banks and/or information technology service providers, electronic banking services, reporting, and other aspects. In 2020, the Financial Services Authority amended this regulatory requirement and issued the Amendment [POJK Regulation No 38/POJK.05/2020](#), which revised the requirements related to data centers and disaster recovery centers.

To further guide commercial banks in implementing information technology risk management, the Financial Services Authority issued [No 21/SEOJK.03/2017 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank](#) in 2017. This regulation formulates corresponding implementing details for each regulatory requirement in No 38/POJK.03/2016, covering various aspects such as management, development and procurement, information technology operational activities, communication networks, information security, disaster recovery plans, and the use of information technology service providers.

In this section, Tencent Cloud summarizes the control requirements relevant to cloud service providers in No 38/POJK.03/2016 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank and its amendments, as well as No 21/SEOJK.03/2017 - The Implementation of Risk Management in The Use of Information Technology by Commercial Bank, and explains how Tencent Cloud, as a CSP, assists commercial banks in complying with these requirements.

5.1 Information Technology Management

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
8		1.7	Adequacy of Policies, Standards, and Procedures for Information Technology Use in Banks	(1) A Bank shall be obligated to establish Information Technology use policies, standards, and procedures, and shall be obligated to implement these policies, standards,	Customers should formulate policies, standards, and processes for the use of information technology, regularly review and update these policies and processes, and set tolerable risk limits to ensure the optimal operation of information technology-related aspects. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which

No. regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
		and procedures consistently and continuously. (2) The Information Technology use policies, standards, and procedures shall cover at least the following aspects: a. Management; b. Development and procurement; c. Information Technology operations; d. Communication networks; e. Information security; f. Disaster Recovery Plans; g. Electronic Banking; h. The use of Information Technology service providers; i. The provision of Information Technology services by the Bank. (3) A Bank shall be obligated to set tolerable risk limits to ensure that the Information Technology-related aspects referred to in Paragraph (2) operate optimally. (4) A Bank shall be	comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			obligated to review and update the policies, standards, and procedures referred to in Paragraph (2) on a regular basis. (5) A Bank shall be obligated to specify the timeframe for reviewing and updating the policies, standards, and procedures referred to in Paragraph (4) in a written policy.	
10	1.8	Risk Management Process Related to Information Technology	(1) A Bank shall be obligated to establish policies, standards, and procedures for the Information Technology risk management process. (2) A Bank shall be obligated to implement a risk management process related to the use of Information Technology. (3) The risk management process referred to in Paragraph (2) shall be implemented for at least the Information	The customer shall formulate and implement policies, standards, and procedures related to information technology risk management processes. The customer shall conduct regular information technology risk assessments, collect information technology activities that may generate or increase risks, perform qualitative and quantitative analyses on identified risks based on their impact levels and occurrence frequencies, confirm the priority of control measures, implement risk mitigation measures, and continuously monitor and track the implementation of control and mitigation activities for identified risks. If the customer engages information technology service providers, it shall ensure that the service providers also implement corresponding risk management processes. To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			Technology-related aspects referred to in Article 8 Paragraph (2). (4) In cases where a Bank uses Information Technology service providers, the Bank shall be obligated to ensure that the Information Technology service providers implement risk management as stipulated in this Financial Services Authority Regulation.	entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Risk Identification: Tencent Cloud conducts risk assessments at least annually, identifying applicable risk scenarios from sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. Risk Assessment: Tencent Cloud evaluates asset value, the likelihood of risk scenarios, and the potential impact, then calculates the risk level. Risk Treatment: Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items, the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored. Risk Monitoring, Review, and Reporting: Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions.

5.2 Information Technology Development and Procurement

No.	Domain	Summary of Controls	Tencent Cloud's Response
11	2.2-2.3 Policies, standards and procedures for development and procurement	In developing and procuring Information Technology, a Bank shall be obligated to implement control measures to ensure that systems and data maintain confidentiality and integrity, and support the achievement of the Bank's objectives. These measures shall include at least the following: a. Establishing and implementing consistent procedures and methodologies for the development and procurement of Information Technology; b. Implementing project management in system development; c. Conducting adequate testing during the development and	When customers carry out information technology development and procurement, they should formulate and implement information technology development and procurement processes and plans, conduct project management, carry out sufficient testing, and retain process documents. In addition, customers should also establish an application system change management mechanism to ensure that information technology systems can be fully traced back. If the software used by the customer is developed by a third party and the source code is not provided, the customer needs to evaluate the necessity of signing a written escrow agreement with the third party. To support customers in R&D management, Tencent Cloud provides Cloud Native Build (CNB) developer tools. CNB is based on the Docker ecosystem, abstracting environments, caches, and plugins, and uses declarative syntax to help developers build software more efficiently. CNB offers a complete developer toolchain with capabilities such as code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and custom task sets, effectively enabling end-to-end R&D process support and agile development management from requirements to deployment.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			procurement of a system (including joint testing with user units) to ensure the system's accuracy, functionality (in line with user needs), and compatibility with other systems; d. Documenting system development and maintenance; e. Establishing application system change management; f. Ensuring the Bank's Information Technology systems can retrieve complete information; g. Assessing the urgency of entering into a written escrow agreement for software deemed critical to the Bank's operational continuity (in cases where the software is developed by a third party and the source code is not provided to the Bank).	Tencent Cloud, as a cloud service provider, on its international portal, Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. To support customers in meeting regulatory requirements, in terms of secure system development, Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls throughout the product lifecycle. Key security measures include: • Security Training: Developers receive secure coding training and are required to follow secure coding guidelines. • Requirements Analysis: Engage in discussions on business content, workflows, and technical frameworks to identify optimal security integration points. • System Design: Perform threat modeling and security assessments of the chosen architecture. • System Development: Provide Tencent-designed secure development components and

No. regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			enforce secure coding practices. • Security Validation: Conduct code security checks, asset scans, web vulnerability scans, manual security assessments, penetration testing, and code audits to identify vulnerabilities. • Release: Systems are deployed to production only after all high-risk issues have been fixed to prevent vulnerabilities from entering the live environment. In terms of system testing, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams. For third-party product usage, Tencent Cloud has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies. In terms of change management, Tencent Cloud has established a set of management standards for

No.		Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules			
				product and configuration changes, all types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment.
N/A	2.4	Risk Measurement for Development and Procurement	(1) At each phase of IT development and procurement, banks must mitigate identified and measured risks using control methods specified in the bank's IT development and procurement policies, standards, and procedures. After mitigation, banks must monitor controlled risks and residual risks—as any disruption affecting IT development and procurement plans or processes may ultimately impact bank operations. (2) To control risks related to IT development, banks must ensure system development complies with policies, standards,	The customer should implement risk management processes for development and procurement, clarify the risk measurement factors for development and procurement, and implement risk mitigation measures for the identified risks. In addition, the customer should formulate policies, standards, and processes for each development stage of the system. If the customer procures the system, they should clarify the supplier selection criteria, evaluate the supplier's capabilities before selecting them, and sign a contract agreement with the supplier to clarify the responsibilities and obligations of both parties. To support customers in meeting regulatory requirements, in terms of risk measurement and risk control, Tencent Cloud has defined an Information Security Risk Management Procedure, which provides clear defines for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessments at least annually, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk

No. regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
		and procedures for each development phase. (3) To control procurement risks, banks must establish vendor selection criteria and evaluate vendor capabilities (e.g., financial condition, support level, security controls) before selecting vendor products or services.	level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. Furthermore, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices. In terms of system development, Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls and evaluation throughout the product lifecycle. In terms of due diligence, Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. The following is an overview of Tencent Cloud's practices as a cloud service provider in responding to due diligence requirements across various aspects: • Technical strengths: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and

No. regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products, ensuring reliable and continuous service for customers. Financial stability: Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant. Service support level: Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services. In terms of contracts and agreements, Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure requirements. Customers can also choose to sign a customized agreement with Tencent Cloud to negotiate and modify specific terms and rules in the agreement. Regarding customers' continuous monitoring and evaluation of Tencent Cloud, in terms of customer audits and regulatory reviews, Tencent

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. To ensure that Tencent Cloud's information technology policies, procedures, processes, and control measures meet the requirements of Indonesian financial regulations, Tencent Cloud engages a third-party auditing firm to conduct an independent audit of its internal control system and issue an IT compliance audit report for the Indonesian financial industry. And Tencent Cloud has also obtained Indonesia's SNI 27001 certification.

5.3 Information Technology Operation Activities

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
12		3.2	Policies, standards and processes for IT operation activities	A Bank shall be obligated to ensure the continuity and stability of Information Technology operations, and mitigate risks that may disrupt the Bank's operational activities.	Customers shall ensure the continuity and stability of information technology operations, and be able to mitigate or reduce the risks that disrupt their business operations. Tencent Cloud has established standardized procedures to guide daily operational activities for operations personnel, including asset management, physical and environmental security management, capacity management, security configuration management, media management, etc.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				Tencent Cloud leverages mature, automated operations management platforms to manage operational tasks and strictly controls change windows through internal mechanisms, ensuring requests are completed within designated timeframes. Detailed operational security “red lines” are defined, and internal security reviews are conducted regularly. To ensure traceability and accountability in production environments, all backend operational activities are thoroughly logged, centralized in the log management platform, and periodically reviewed by Tencent Cloud’s internal audit team to identify and investigate suspicious actions.
21	N/A	Placement of Electronic Systems in Data Centers and/or Disaster Recovery Centers	(1) A Bank shall be obligated to place its Electronic Systems in Data Centers and Disaster Recovery Centers within the territory of Indonesia. (2) A Bank may only place its Electronic Systems in Data Centers and/or Disaster Recovery Centers outside the territory of Indonesia with the approval of the Financial Services Authority.	The customer shall place its electronic systems in data centers and disaster recovery centers located within the territory of Indonesia. If the customer places its electronic systems in data centers outside Indonesia, it shall submit legal documents such as national risk analysis, statement documents, and cooperation agreements to obtain approval from the Financial Services Authority. Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options and strictly complies with applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Customers may flexibly deploy data and systems across different regions or availability zones based on business needs and data security requirements. Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
22	3.2.1	Policies related to data centers		cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia.
				Customers should formulate policies, standards, and procedures related to data center operational activities, implement physical access control for data centers, and protect the physical environment security of data centers to ensure that data centers and disaster recovery centers can guarantee the continuous operation of business.
			The Data Centers and Disaster Recovery Centers shall be obligated to ensure the Bank's business a. Data Center Operational Activities; b. Physical Access Controls for Data Centers; c. Data Center Environmental Controls	To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, organized by regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. As a cloud service provider, Tencent Cloud is committed to delivering secure, stable, continuous, and reliable physical infrastructure for customers. Currently, Tencent Cloud operates three leased data centers in the Indonesia region. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. Customers can flexibly deploy data and systems across different regions or availability zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures. Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network

No.				
regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				services even in the event of single-point device failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts annual on-site audits to verify that data center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures. In terms of physical environment management, Tencent Cloud ensures that all global data centers are selected, constructed, or leased in compliance with relevant international standards and local security requirements. For leased data centers in the Indonesia region, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity, Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				data center. For physical access control, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. For physical and environmental incidents, Tencent Cloud requires operators to establish escalation mechanisms, response plans, and handling procedures, and to conduct regular drills to validate these processes. This ensures rapid response and resolution of such incidents,

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
12	3.2.2	Policies for IT Capacity Planning and Monitoring		minimizing their impact on Tencent Cloud's platform and services.
				Customers should establish a mechanism for IT capacity planning and monitoring, continuously monitor the usage of system resources, set performance and capacity thresholds, and implement necessary processes to manage situations where the preset thresholds are exceeded.
			Banks must establish policies and procedures for IT capacity planning and monitoring to ensure that the hardware and software used align with business operational needs and anticipate the bank's business development. Without sound IT capacity planning, banks may face risks of resource shortages or even waste of IT resources. IT capacity planning must be developed for a sufficiently long timeframe and regularly updated to accommodate existing changes.	To support customers in efficient capacity planning and adjustment, Tencent Cloud provides Auto Scaling (AS) services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs, policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. To enable effective monitoring and management of system performance, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services.
12	3.2.3	Policies for Hardware and Software Configuration Management	Banks must establish procedures related to: - The installation process for hardware and software; - The parameter configuration (hardening) of hardware and software; - The inventory and update of information on hardware, software, network infrastructure, storage media, and other support equipment located in the Data Center.	Customers should inventory their hardware, network infrastructure, storage media, and software, and update them regularly. Customers should also implement security hardening configurations for hardware and software. To assist customers in comprehensive information asset management, Tencent Cloud provides Cloud Workload Protection Platform (CWPP), which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, Cloud Security Center (CSC), for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				as cloud configuration risks, vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. Tencent Cloud's Cloud Security Center (CSC) provides automated configuration risk assessment capabilities to help customers reduce security risks caused by misconfigurations and improve overall cloud security posture. To support customers in meeting regulatory requirements, Tencent Cloud has established information asset management standards and lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems. Tencent Cloud has established a Configuration Management Policy and uses a Configuration Management Database (CMDB) to centrally manage IT service components and configuration items (CIs), including their relationships. When configuration updates occur during change processes, operations personnel update the version and related information of configuration items in the CMDB according to the change plan. Tencent Cloud conducts regular asset inventories and audits the CMDB to ensure the validity, accuracy, and completeness of configuration information. Tencent Cloud has established configuration and baseline standards to standardize security settings for network devices, firewalls, servers, operating systems, databases, and applications.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
12	3.2.4	Policies for Hardware and Software Maintenance	a. Regular preventive maintenance of IT equipment is required to minimize operational failures of the equipment and detect potential issues early. For this purpose, banks must establish maintenance agreements with vendors to ensure the availability of maintenance support. Maintenance must be based on established schedules, documented in a logbook, and reviewed regularly. b. Monitoring of hardware and software must be conducted daily to ensure all such equipment operates as intended. Examples include ensuring servers remain powered on, database and server utility capacity does not exceed limits, and support facilities function properly.	Continuous scanning tools detect deviations from standards in operating systems, database management systems, and virtual images. Identified deviations automatically generate security tickets for timely remediation. Security teams also review network device policies and parameters regularly to ensure effectiveness. Customers should conduct preventive maintenance on IT equipment to reduce equipment operational failures, sign maintenance agreements with equipment suppliers, and carry out maintenance as planned. In addition, customers should also monitor the normal operation of hardware and software. Regarding the maintenance of Tencent Cloud hardware and software used by customers, Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud offers online chat and telephone support via the cloud console and official website, allowing customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates geographically redundant customer service centers, providing 24/7 support to handle customer requests, deliver round-the-clock technical assistance for cloud products, and ensure timely, high-quality service responses. Customers may also select an appropriate support plan, which can include access to dedicated support groups, a designated technical account manager, and value-added services for enhanced assistance.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				To support customers in meeting regulatory requirements, Tencent Cloud maintains a detailed inventory of hardware and facilities in its Configuration Management Database (CMDB), including each server's End-of-Support (EOS) date and version information. Tencent Cloud regularly retires and replaces servers, while software components (such as operating systems and database systems) are upgraded to appropriate versions before reaching end-of-support. For decommissioned hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction in official logs. In terms of infrastructure maintenance and monitoring, Tencent Cloud assigns on-site data center personnel to regularly inspect critical equipment in server rooms, following predefined procedures to record inspection results, report anomalies, and resolve identified issues promptly to eliminate security risks and ensure stable operation of equipment. Tencent Cloud also deploys monitoring systems to continuously track key metrics of critical data center equipment 24/7. In case of anomalies, alerts are automatically sent to on-site personnel.
12	3.2.5	Change Management Policies	Banks must establish change management policies, standards, and procedures that cover, at minimum, request submission, analysis, change approval, and change implementation—including the transfer of hardware and software from the testing	The customer shall formulate a change management procedure, and changes to information assets shall be evaluated, tested, reviewed, and approved before implementation. In addition, in change management, the customer shall retain complete records of patch installations. When customers conduct data migration in the event of material changes to their application systems or the need to consolidate data from multiple disparate systems, they shall establish policies, standards

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				environment to the operational environment. a. Procedures for change implementation must consider operational continuity in the operational environment, oversight, and information system security settings. The established minimum standards must cover risks, testing, authorization and approval, implementation timing, post-installation validation, and back-out or recovery plans; b. In change management, banks must maintain complete documentation of patch installations. Additionally, banks must ensure they use the most appropriate latest version of software. Banks must also maintain up-to-date information on product fixes, security issues, patches or upgrades, or other issues relevant to the software version in use; c. Data migration occurs when there are	and procedures for data migration. To support customers in meeting regulatory requirements, in terms of change management, Tencent Cloud has established product and configuration change management standards defining all steps and responsible parties in the change process to ensure proper approval and testing before implementation. Emergency changes follow a dedicated management process and require appropriate approval prior to execution. All program changes—including application, configuration files, operating systems, and databases, must undergo business impact analysis, have rollback plans in place, and be approved by responsible personnel before deployment. Tencent Cloud's change release system enforces that only authorized personnel can execute changes, retain change-related logs, and conduct regular log reviews. After release, Tencent Cloud operations team monitors changes in the production environment and records results. Tencent Cloud classifies change requests based on attributes such as importance, urgency, and scope of impact. For changes that may affect external environments—such as product, infrastructure, or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels. For patch management, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. If customers need to terminate the

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				significant changes to application systems or when data is merged from multiple different systems. In cases involving data migration, banks must establish policies, standards, and procedures for managing data migration.	contractual agreement due to business changes or future IT planning , they may choose to back up and migrate cloud data and production environments at any time. Tencent Cloud's products support customers in backing up or migrating data using common standard formats. This enables customers to adopt the same transmission methods and protocols used during cloud onboarding, or leverage network services such as Direct Connect (DC) and VPN Connection to ensure secure and reliable data transfer during termination of cloud service engagement.
12		3.2.6	Incident or Problem Handling Policies	Sound incident or problem handling procedures are necessary for banks to address financial, operational, and reputational risks arising from issues. Incident or problem handling procedures must cover hardware, operating systems, application systems, network equipment, and security equipment. Banks must maintain the necessary resources to handle issues, including: a. Banks must establish a helpdesk function to promptly respond to and resolve issues faced by all users within the bank. Banks will face risks if they lack adequate helpdesk procedures to	Customers should establish a sound process for handling incidents and issues to address various security risks caused by problems. In terms of issue management, Tencent Cloud has implemented problem management standards that leverage event data and trend analysis to identify root causes and develop solutions, minimizing the impact of incidents and problems on business operations. Tencent Cloud centrally manages knowledge related to problem resolution to improve handling efficiency and adopts preventive measures to avoid repeated incidents, thereby enhancing service quality. For incident management, Tencent Cloud has established incident and service request management procedures and formulated an incident management policy. This ensures that all incidents related to IT service management activities are recorded and categorized, prioritized based on impact and urgency, and escalated as needed to ensure rapid resolution and closure. These measures minimize the impact of incidents, maintain normal business operations, and enhance customer satisfaction. Tencent Cloud also provides multiple

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			ensure users receive solutions to their problems; b. For issue handling, banks must establish procedures for managing power users to prevent misuse.	channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services. In terms of privileged account management, <u>Cloud Access Management (CAM)</u> provides granular permission control, allowing customers to assign specific permissions to different personnel for different resources. In addition, customers can use <u>CloudAudit</u> to monitor Tencent Cloud account activities, perform compliance checks, operational reviews, and risk audits. CloudAudit supports online viewing of Tencent Cloud console and cloud API operation records for up to 90 days. Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
12	3.2.7	Database Management Policies		Banks must classify the sensitivity of information stored in Databases as a basis for oversight. Databases storing confidential information require stricter controls than those storing non-sensitive information. For this purpose, banks must have a Database Administrator (DBA) responsible for managing the bank's Databases. Bank procedures related to Databases include Database access, maintenance, problem handling, and administration.	Customers should classify the information stored in the database according to its sensitivity and implement strict controls on databases that contain sensitive information. In addition, customers should also appoint database administrators to manage database access, maintenance, and problem handling. Tencent Cloud provides Tencent Cloud Enterprise (TCE), a self-developed private version based on Tencent's mature public cloud system. It helps customers build a fully autonomous, controllable, elastic, and scalable full-stack digital infrastructure for the era of large models, offering one-stop solutions for enterprise digital operations. With strong product capabilities and professional services, it assists customers in the financial sector in achieving rapid cloud migration as well as efficient operation and maintenance. The Data Security Governance Center (DSGC) helps customers automatically identify and classify cloud-based data assets and assess associated security risks. DSGC is an integrated data security operations platform that supports sensitive data discovery, classification and grading, data mapping, and abnormal access analysis. It works in coordination with Tencent Cloud's security capabilities to form a closed-loop data protection framework, maximizing security effectiveness for enterprises. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps

No.				
regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access Customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with applicable laws and regulations during investigations by national or local authorities. Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services, and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities. Tencent Cloud's internal office network is completely isolated from the production environment where Customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-factor authentication. To protect the confidentiality and integrity of Customer data, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength cryptographic algorithms. These products integrate with the Key Management Service (KMS) to provide

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					full lifecycle management of encryption keys, ensuring data confidentiality.
12		3.2.8	Information Exchange Control Policies	Banks must establish procedures for managing the physical and logical transmission of information, including: a. Requests for and provision of information by internal and external parties; b. Information transmission via various media (e.g., hardcopy, tapes, disks, email, mail, and the internet). For large banks with high IT complexity, management must consider segmenting Wide Area Networks (WAN) and Local Area Networks (LAN) using security equipment (e.g., firewalls) to restrict access and data traffic flow.	Customers should establish physical and logical information transmission management processes to properly manage the application for and provision of internal and external information, as well as information transmission through various media. For large bank customers with high IT complexity, consideration may be given to using security devices for segmented network management to restrict data access and the inflow and outflow of traffic. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • <u>Direct Connect (DC)</u>: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • <u>VPN Connection</u>: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • <u>Cloud Connect Network (CCN)</u>: Enables private network interconnection between cloud VPCs and between VPCs and on-premises data centers (IDCs).

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				CCN supports full-mesh connectivity, dynamic route learning, optimal path selection, and fast convergence in case of link failures. All communication within CCN remains on private networks without traversing the public Internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further guarantees communication quality, making data transmission secure and reliable. For banking customers with high IT complexity, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. To implement network perimeter protection to restrict data access and the inflow and outflow of traffic, Tencent Cloud offers the EdgeOne (EO) platform, which provides security and acceleration services through Tencent's global edge nodes. EO includes DDoS protection, intelligent web defense, bot/crawler attack mitigation, DNS resolution, and supports custom access control rules. Customers can also use Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services.

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					• Cloud Firewall (CFW) provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. • Web Application Firewall (WAF) helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. • Anti-DDoS combines abundant, high-quality DDoS mitigation resources with continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks, ensuring stable and secure business operations.
12		3.2.9	Library Management Policies	Library managers are responsible for inventorying and storing all software and data stored on various media (e.g., tapes and disks). Additionally, library managers must store copies of all policies and procedures—such as Data Center-related run book manuals. When developing policies, standards, and procedures for libraries, banks must ensure adequate procedures for media storage, backup, and disposal. Backups of data and programs must be regularly updated to	The customer shall establish a warehouse administrator position, who shall be responsible for the inventory and storage of all software and data stored in various media, as well as for maintaining all policies and processes. In addition, the customer shall have policies and procedures for media storage, backup, and disposal, and backups of data and programs shall be updated regularly. To support customers in meeting regulatory requirements, Tencent Cloud has established standardized procedures to guide daily operational activities for operations personnel, including physical and environmental security management, media management, backup management, etc. In terms of media management, Tencent Cloud stores and disposes of media according to the sensitivity level of the information stored in the media, and has established media management-related procedures, specifying the

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				ensure the bank can recover systems, applications, and data in the event of a disaster or other disruption.	specific processes and standards for media storage and media disposal. Relevant approval is required before media disposal, and records of the disposal process should be made. Depending on the material, storage principle, and sensitive information level of the different media, the relevant teams will choose targeted disposal methods to ensure that the data cannot be recovered and complies with safety regulations. Regarding the redundancy and backup management of the library, Tencent Cloud data centers span multiple regions worldwide, including Mainland China, Asia-Pacific, North America, and Europe, organized into regions and availability zones. Customers can flexibly deploy data and systems across different regions or zones according to business needs and security requirements, adopting various business continuity models to meet disaster recovery objectives. Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia. Tencent Cloud's compute, network, storage, database, container, and middleware services provide highly available architectures and support customer-defined backup strategies to meet diverse backup needs.
12		3.2.10	Hardware and Software Disposal Policies	Activities that banks need to be conducted include: a. Migrating data from production systems to backup media using procedural	Customers shall promptly delete data stored on hardware and software that is no longer in use or has exceeded the retention period, migrate data from production systems to backup media in accordance with established procedures and mechanisms, archive data based on the retention period, and dispose of data that has

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			mechanisms—including testing and backup procedures; b. Storing system documentation as preparation for potential re-installation of a system on production servers; c. Managing data archives in accordance with retention periods; d. Disposing of data that has exceeded its retention period.	exceeded the retention period. A variety of storage and database services provided by Tencent Cloud are equipped with backup capabilities to meet customers' diverse backup requirements. Examples are as follows: • Data stored by customers in Cloud Object Storage (COS) can be replicated across multiple designated regions through the cross-region replication feature, ensuring that complete data can still be retrieved and restored from redundant copies in case of accidental partial data loss. This also prevents losses caused by unavoidable disasters affecting storage in a single availability zone, achieving the effect of multi-redundancy backup and remote disaster recovery. • The snapshot backup feature of Cloud Block Storage (CBS) backs up data by capturing point-in-time snapshots of CBS, preventing data loss caused by tampering or accidental deletion and enabling quick rollback in the event of service failures. • Cloud File Storage (CFS) offers a scheduled snapshot feature, allowing customers to flexibly configure backup policies. It is recommended that customers adopt different scheduled snapshot policies for different business scenarios. • TDSQL-C for MySQL, the cloud-native database, supports two backup types: logical backup and snapshot backup. With full data backups plus subsequent binlog backups over a period of time, the entire TDSQL-C for MySQL cluster or specific databases and tables can be

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				restored to any point in time. • TencentDB for MySQL supports both automatic and manual database backup methods, and provides cross-region backup capabilities to help customers enhance their disaster recovery capabilities and improve data reliability. • TencentDB for MongoDB is equipped with an automatic data backup and lossless recovery mechanism, supporting multi-node data backup. Customers can retain backup data for multiple days through this mechanism to facilitate data recovery in disaster scenarios. In addition, Tencent Cloud Data Transfer Service (DTS) supports the migration of multiple relational databases and NoSQL databases such as MySQL, MariaDB, PostgreSQL, Redis, and MongoDB. It enables users to seamlessly migrate databases to the cloud without interrupting business operations, easily build a highly available database disaster recovery architecture through real-time synchronization channels, and meet scenario-specific requirements such as commercial data mining and asynchronous business decoupling via data subscription. Cloud Migration (CMG) integrates a variety of migration tools and provides unified monitoring. During the migration process, users can choose either Tencent Cloud's official migration tools or officially certified third-party migration tools. Cloud Migration helps users migrate systems to the cloud in a convenient and efficient manner while allowing them to clearly track migration progress. Furthermore, Tencent Cloud also offers Migration Solution, helping enterprises migrate to Tencent Cloud services in a cost-effective and highly efficient

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
			way. By leveraging Tencent Cloud's high-performance, secure, and stable cloud products and services, it empowers the growth of customers' businesses. If customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate cloud data and production environments at any time. According to the service agreement between Tencent Cloud and the customer, if the cloud service expires or is terminated, customers must complete data migration before the retention period ends for any data stored on cloud servers through Tencent Cloud services. Tencent Cloud support customers in backing up and migrating data using common standard formats. Customers can use the same transmission methods and protocols as during onboarding or leverage network services such as Direct Connect (DC) and VPN Connection to ensure secure and reliable data transfer during offboarding. After cloud services are terminated, Tencent Cloud will follow strict data erasure procedures and permanently delete all customer data, including replicas and backups, after the retention period. Deleted data cannot be restored.

5.4 Information Technology Communication Network

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
13	4.2	Policies, Standards, and Procedures for Banks have the obligation to provide communication networks that meet the principles of	Customers shall provide communication networks that comply with the principles of confidentiality, integrity, and availability, and formulate policies, standards, and procedures to guide the construction of such networks.

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			Communication Networks	confidentiality, integrity, and availability. Banks must establish policies, standards, and procedures as guidelines for providing communication networks—ensuring the continuity of operations and the security of communication networks are maintained.	Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures. Similarly, Tencent Cloud's compute nodes adopt a redundancy design, and any faulty node is automatically removed by the scheduler in real time, ensuring service continuity for Customer workloads. In terms of network communication security, all communications on the Tencent Cloud Console are encrypted using the HTTPS protocol. Tencent Cloud's cloud API interfaces provide HTTPS encryption, signature verification, and status monitoring to ensure port-level communication security for customer operations. Direct Connect (DC) offers dedicated, high-security, high-bandwidth network connections, enabling customers to use exclusive network links and reduce data leakage risks. Customers can also use Cloud Connect Network (CCN) to establish secure private interconnections between VPCs or between VPCs and on-premises data centers (IDCs).
13		4.3.1	Communication Network Risk Management Process	To control risks in communication networks, banks must consider the following: 1. Communication network design; 2. Access control; 3. Operation and maintenance of communication networks; 4. Document record.	Customers should design communication networks with a balance of efficiency and flexibility, implement access control for communication networks, carry out the operation and maintenance of network communications, and retain relevant documents. Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures. Similarly, Tencent Cloud's compute nodes adopt a redundancy design, and any faulty node

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				is automatically removed by the scheduler in real time, ensuring service continuity for Customer workloads. In terms of network communication security, all communications on the Tencent Cloud Console are encrypted using the HTTPS protocol. Tencent Cloud's cloud API interfaces provide HTTPS encryption, signature verification, and status monitoring to ensure port-level communication security for customer operations. Cloud Access Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. Direct Connect (DC) offers dedicated, high-security, high-bandwidth network connections, enabling customers to use exclusive network links and reduce data leakage risks. Customers can also use Cloud Connect Network (CCN) to establish secure private interconnections between VPCs or between VPCs and on-premises data centers (IDCs). In response to the requirements for network partitioning, Customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources, with customizable IP ranges and routing policies. VPC uses tunneling technology to build virtual networks on physical infrastructure, achieving complete logical isolation between private networks. Within a VPC, customers can configure security groups and network ACL rules to control inbound and outbound traffic at both instance and subnet levels, enabling multi-layered

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				network access control. To implement network boundary protection, Tencent Cloud provides the EdgeOne (EO) platform, which leverages Tencent's global edge nodes to deliver security and acceleration services, including DDoS protection, intelligent web defense, bot/crawler attack mitigation, and DNS resolution. EO also supports custom access control rules based on business needs. Customers can further enhance perimeter security using Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services. Cloud Firewall (CFW) offers ACL-based firewall control, IPS real-time interception, virtual patching, and malicious code detection, enabling granular isolation between VPCs and protecting core assets. Web Application Firewall (WAF) defends against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and malicious crawlers. Anti-DDoS combines abundant mitigation resources with AI-driven traffic cleansing algorithms to counter evolving DDoS threats. In terms of network security control management, Tencent Cloud has also established internal network security management specifications and a network in-depth defense system. Through formal policies and procedures, Tencent Cloud defines network security controls, protection standards, and the roles and responsibilities of relevant personnel to ensure the secure operation of services hosted on its network. Tencent Cloud has deployed a mature network security architecture. Through multiple protection mechanisms such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, network logical isolation, and Web application security, it can promptly detect, filter, and block

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				malicious network traffic to protect the network security of Tencent Cloud. In addition, Tencent Cloud ensures that unauthorized personnel are prohibited from accessing any internal network resources, including network analysis and monitoring tools, through corresponding permission control and approval processes.
13	4.3.2	Risk Monitoring	Monitoring of potential risks in the communication networks used by banks must include: a. Regularly monitoring available audit trails to detect anomalies early; b. Periodically measuring network performance based on availability levels and response times; c. Monitoring used and required capacity (for business development plans) compared to installed capacity; d. Monitoring and following up on network intrusions or attacks; e. Conducting regular reviews of user access rights to ensure alignment with roles and authorities. Additionally, reviewing bank users with access to external communication networks is required.	Customers shall establish a continuous risk monitoring mechanism to conduct real-time monitoring of potential risks in communication networks. Specific measures include: periodically reviewing available audit records to identify abnormal activities at an early stage; continuously measuring network performance indicators to ensure service stability; monitoring capacity utilization to optimize resource allocation; and proactively detecting network intrusions and attacks and taking timely response measures. For log management, to assist customers in collecting, compiling, and analyzing evidence related to incidents, Tencent Cloud provides the Cloud Log Service (CLS) to assist customers in collecting, aggregating, and analysing event-related evidence. CLS is designed with a highly available distributed architecture and stores log data with multiple redundant backups to prevent data loss in the event of a single-node failure, ensuring service availability and reliability. In addition, Tencent Cloud's Elasticsearch Service (ES) is deployed within logically isolated Virtual Private Clouds (VPCs), allowing customers to fully control their environment configurations, customize network access control lists and security groups, and leverage multi-availability zone deployment options to maintain service continuity even during network or power outages in a single zone.

No.				
regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				For network log collection and retention, Cloud Firewall (CFW) supports full traffic analysis and can retain logs for up to six months. It also provides advanced threat tracing capabilities, including analysis of domain registration, resolution, filing, and historical DNS information. To support regulatory compliance, Tencent Cloud has established comprehensive log collection and management standards covering the recording, extraction, storage, protection, analysis, and auditing of login logs, operation logs, system logs, and security event logs. All logs are centralized on Tencent Cloud's log management platform and protected with strict backup and security measures to prevent unauthorized modification or deletion. Tencent Cloud uses automated operational security auditing tools and an internal audit team to review logs regularly, detect anomalies, and mitigate operational risks. To enable effective monitoring and management of system performance and capacity, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console. In terms of regular review of user permissions, Tencent Cloud, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. In terms of regular review of user permissions, Tencent Cloud regular internal access reviews are conducted to ensure that privileges are not misused or abused. Access rights that are no longer required are promptly revoked through appropriate follow-up actions.

5.5 Information Security

No.		Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules			
16	5.2.1-5.2.2	Information security policies and standards	Bank management must establish information security policies and demonstrate strong commitment to them. These policies must align with the bank's risk appetite and be regularly communicated to all bank employees and relevant external parties. Additionally, policies must be regularly evaluated, and updated if significant changes occur. Bank management must establish information security standards in line with information security policies, with reference to legal regulations and best practices.	The customer's senior management shall formulate information security policies that align with the customer's risk appetite, demonstrate a high level of commitment to these policies, and communicate them to all employees and relevant stakeholders on a regular basis. In addition, based on these information security policies, the customer shall develop information security standards with reference to applicable laws, regulations and industry best practices. The information security policies shall also be reviewed and updated periodically. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				Tencent Cloud conducts information security and personal data protection training for all business units at least once a year and requires personnel to confirm annually that they have read and understood security policies and procedures.
16	5.2.3.1	Asset Management Procedures	Asset management procedures must include at minimum: a. Bank assets related to information must be identified, their owners or custodians designated, and documented to ensure proper protection; b. Assets related to information may include data (hardcopy or softcopy), software, hardware, networks, support equipment (e.g., power supplies and air conditioners), and HR (including qualifications and skills); c. Rules for information and asset usage must be identified, documented, and implemented. All bank employees and third parties must comply with these rules—such as those governing the use of email, the internet, mobile devices, teleworking, and other tools;	Customers should maintain an inventory of all information assets and establish an information asset management mechanism to identify, classify, and assign ownership of assets. Security controls should be applied based on the classification level of each asset. The asset inventory should be reviewed regularly and updated promptly whenever changes occur. To assist customers in comprehensive information asset management, Tencent Cloud provides Cloud Workload Protection Platform (CWPP), which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, Cloud Security Center (CSC), for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such as cloud configuration risks, vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. Customers can use the Data Security

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			d. Information must be classified to enable appropriate security measures based on its classification. Classification may be based on value, confidentiality level, legal requirements, and importance to the bank.	<u>Governance Center (DSGC)</u> helps customers automatically identify and classify cloud-based data assets and assess associated security risks. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. To support customers in meeting regulatory requirements, Tencent Cloud has formulated information asset management specifications and full-lifecycle management processes, which conduct classified and hierarchical management and protection of assets such as electronic data, hardware and their virtual devices, infrastructure, application systems, and software. Tencent Cloud manages hardware devices and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, etc. This ensures the stable operation of the underlying system of the cloud platform and provides reliable support for business systems. Tencent Cloud has also implemented an Acceptable Use Policy, which clearly defines the responsibilities and obligations of employees and third parties when using Tencent Cloud resources (including but not limited to IT systems, networks, devices, and data). This policy regulates appropriate usage and mitigates potential risks.
16	5.2.3.2	Human Resource	HR management procedures must include	Customers should properly manage personnel who have access to information, such as

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			Management Procedures	at minimum: a. Banks must implement adequate controls before hiring IT employees (permanent, contract, or freelance), consultants, or IT service provider staff for roles that pose vulnerabilities or significant impacts on information security. For example, conducting background checks for criminal records or offenses like data theft during recruitment for network administrator or system administrator positions; b. HR (including bank employees, consultants, freelancers, and IT service provider staff) with access to information must understand their responsibilities for information security; c. The roles and responsibilities of HR (including bank employees, consultants, freelancers, and IT service provider staff) with access to information must be defined based on their information access	establishing a personnel selection process, signing confidentiality agreements with employees, conducting publicity and education on information technology risk awareness, formulating disciplinary measures for violations, and establishing management mechanisms for resignation or job transfers. To support customers in meeting regulatory requirements, Tencent has established comprehensive HR management standards and procedures to ensure personnel are selected, recruited, and assigned according to job requirements. Tencent Cloud has implemented a clear employee lifecycle management process, including onboarding, employment, and offboarding procedures. Before employment, applicants undergo interviews to assess their suitability for the role. Based on applicable laws and job level, the HR department conducts background checks prior to hiring. These checks include verification of past employment history, criminal background, and academic qualifications. The results are recorded in Tencent Cloud's HR management system. Upon employment, internal staff must sign an employment agreement and a confidentiality agreement. The employment agreement specifies Tencent Cloud's security policies and the responsibilities of employees or third-party personnel regarding information security and personal data protection. The confidentiality agreement outlines confidentiality obligations and penalties for violations. Outsourced staff are also subject to background checks and bound by employment and confidentiality requirements stipulated in agreements between Tencent Cloud and the outsourcing vendor. Legal teams review and update confidentiality

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			needs and documented in line with information security policies; d. Agreements with bank employees, consultants, freelancers, and IT service provider staff must include IT security provisions aligned with the bank's information security policies. For example, a clause requiring them to maintain the confidentiality of information based on its classification; e. In addition to agreements between the bank and IT service providers, all IT service provider staff assigned to the bank must sign a non-disclosure statement—including confidentiality commitments for customer data protection; f. Information security training and/or socialization must be provided to bank employees, consultants, freelancers, and IT service provider staff. This training must align with their roles and responsibilities;	requirements as needed. Tencent Cloud provides a series of information security training and awareness programs to educate employees on security policies, procedures, and standards. Employees are required to participate in regular information security awareness training. The offboarding process includes timely termination of user accounts and access rights, as well as retrieval of company assets. All physical assets are assigned to designated custodians and registered in Tencent Cloud's internal asset tracking system. Tencent Cloud conducts regular asset inventories to verify asset existence and record results. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			g. Banks must establish sanctions for HR violations of information security policies; h. Banks must establish procedures for requiring the return of assets and the modification or revocation of access rights for bank employees, consultants, freelancers, and IT service provider staff—due to role changes, contract expiration, or termination.	
16	5.2.3.3	Physical and Environmental Security Procedures	Physical and environmental security procedures must include at minimum: a. Critical information processing facilities must be provided with adequate physical and environmental security to prevent unauthorized access, damage, and other disruptions; b. Physical and environmental security for critical information processing facilities includes measures such as room restrictions, access control, on-site security equipment (e.g., alarms, fire detection and suppression	Customers should establish physical and environmental security control mechanisms for information processing facilities, and implement security protection and regular maintenance procedures for hardware equipment and IT-related infrastructure. Tencent Cloud ensures that all global data centers are selected, constructed, or leased in compliance with relevant international standards and local security requirements. For leased data centers in the Indonesia region, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity,

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			systems, temperature and humidity monitors, and CCTV cameras), and maintenance of room and equipment cleanliness (protecting against dust, smoke, food, drinks, and flammable items); c. Support facilities (e.g., air conditioners, power supplies, and fire alarms) must have sufficient capacity and availability to support the operation of information processing facilities; d. IT service provider-owned assets (e.g., servers and switching tools) must be clearly identified and adequately protected; e. Regular maintenance and inspection of information processing facilities and support facilities in accordance with established procedures.	Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the data center. For physical access control, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Tencent Cloud requires data center operators to regularly review access permissions to the data center, follow access procedures, verify the identities of personnel entering the data center, and inspect and register the items they carry. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. For physical and environmental incidents,

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					Tencent Cloud requires operators to establish escalation mechanisms, response plans, and handling procedures, and to conduct regular drills to validate these processes. This ensures rapid response and resolution of such incidents, minimizing their impact on Tencent Cloud's platform and services.
16		5.2.3.4	Access Control Procedures	Access control procedures must include at minimum: a. Physical and logical access controls; b. Banks must implement identification and authentication methods based on risk analysis. c. Banks must have formal, written, and management-approved procedures for user administration—including registration, modification, and deactivation of users (both internal and external, such as vendors or IT service providers); d. Access must be granted based on business needs and follow the principle of least privilege; e. Banks must establish procedures for issuing initial passwords or PINs to users;	Customers should establish identity authentication and access control mechanisms for data and information technology systems to manage access to information assets, and regularly review and update permissions. In terms of user account and authorization management, Cloud Access Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources. Through the CAM console, customers can configure password policies for sub-users, including complexity, length, and validity period. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to customer passwords, ensuring that plaintext passwords are never stored. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. Tencent Cloud has also implemented an access control authorization policy and a role-separation matrix mechanism. It requires user accounts to use unique identifiers and sets password policies for employee accounts based on security baselines, including password length, complexity, locking, and resetting. For internal terminals, operating systems, applications, and network devices, Tencent Cloud has configured policies for limiting the

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			f. Banks must require users to Maintain the confidentiality of passwords or PINs; Choose high-quality passwords or PINs; g. Banks must deactivate access rights for user-IDs unused for a specified period, set a maximum number of failed login attempts, and lock users out after reaching this maximum; h. Banks must conduct regular reviews of user access rights by units independent of access control operations—to ensure alignment with assigned authorities; i. Operating systems, application systems, databases, utilities, and other bank-owned devices must support password or PIN security; j. Banks using file sharing must establish access restrictions—at minimum via password/PIN protection and authorization settings for eligible users.	number of failed login attempts and session timeouts. Tencent Cloud uses a zero-trust security management system to authenticate employee access, requiring users to complete two-factor authentication through the system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions to employees only based on job responsibilities and business necessities. Regular permission reviews are conducted to prevent permission misuse and abuse. For high-privilege users, Customers can use Cloud Access Management (CAM) to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Tencent Cloud has also clearly defined the management requirements for special access permissions and established relevant authorization mechanisms. Tencent Cloud's production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					accessing bastion hosts, and only authorized personnel can log in after completing secondary identity verification.
16		5.2.3.5	IT Operational Security Procedures	IT operational security procedures must include at minimum: a. Banks must maintain records of antivirus and software versions used, regularly monitor information about patches, upgrades, or other issues relevant to the used versions, and conduct evaluation, testing, and installation of these updates; b. Banks must define log types (e.g., administrator logs, user logs, or system logs), data to be included in logs, and retention periods-to support future investigations and access control monitoring; c. Banks must conduct regular reviews of audit trails or logs based on risk analysis—at the network, operating system, database, and application levels; d. Audit trails or logs must be protected against tampering and unauthorized access;	The customer should establish IT operation security processes, including patch management, log management, and physical media management. In addition, the customer should regularly review the IT operation services provided by the IT service provider. For patch management, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Tencent Cloud also operates internal vulnerability scanning and external vulnerability reporting platforms to track and remediate issues. Security tickets are logged in the operations system and assigned to responsible teams for timely resolution. Tencent Cloud's security research team integrates virtual patching capabilities into its Web Application Firewall to enhance overall platform security. To assist customers in collecting, consolidating, and analyzing incident-related evidence, Tencent Cloud provides Cloud Log Service (CLS). As a one-stop log service platform, CLS offers capabilities from log collection and storage to retrieval, real-time consumption, and delivery, helping customers address challenges in business operations, security monitoring, log auditing, and analysis. CLS adopts a highly available distributed architecture with multi-redundant backup storage to prevent data unavailability caused by single-node failures, ensuring service reliability and stability for log data.

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			e. Timestamps for all bank electronic systems must be synchronized with an agreed-upon accurate time source; f. Banks must conduct regular reviews of IT operational services provided by IT service providers. Review intervals must be specified in the service agreement between the bank and the provider; g. Banks must implement controls for physical media in transit—to protect media from unauthorized access, misuse, or damage during transportation outside the bank's physical premises.	<u>Cloud Security Center (CSC)</u> supports the collection of various cloud security-related data, including alerts from security products, cloud asset configuration changes, user activity logs, and selected product logs. CSC provides a unified search and investigation platform to enable comprehensive cloud log auditing and investigation. <u>Elasticsearch Service (ES)</u> aggregates real-time logs from cloud servers, containers, and other cloud products, as well as historical and incremental business data, into Tencent Cloud ES clusters for distributed storage, query, and analysis. To support customers in meeting regulatory requirements, Tencent Cloud centrally collects and manages logs such as login logs, operation logs, system regular logs, and system security event logs on the Tencent Cloud Log Management Platform. It also implements backup and strict protection measures for relevant log information to prevent unauthorized modifications and deletions. Tencent Cloud audits logs through operation and maintenance security automation audit tools and an internal audit team to detect system or operational abnormalities, thereby preventing operational risks. Tencent Cloud ensures that the clocks of relevant facilities are synchronized with accurate time sources, and each data center also regularly checks the time synchronization status of its NTP servers. Regarding the management of in-transit physical media, Tencent Cloud tracks the entire process of media's outbound, transportation and inbound through work orders. During the transportation process, Tencent Cloud selects safe and reliable transportation providers, implements protective measures according to the information level, and provides protective packaging for physical media to prevent

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
					physical damage during transportation. To comply with the customer's outsourcing supervision requirements, Tencent Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual independent professional audits by domestic and international third parties. Through System and Organization Controls (SOC) reports, Tencent Cloud provides assurance to cloud customers, independent auditors, regulators, shareholders, and other stakeholders regarding its latest internal control status. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Indonesian financial regulations, Tencent Cloud engages third-party audit firms annually to perform independent audits of its internal control framework and issues the Indonesian Financial Industry IT Compliance Audit Report.
16		5.2.3.6	Information Security Monitoring Procedures	Banks must conduct monitoring to detect threats to information security—using methods determined by the risk level or	Customers should establish the capability to detect cybersecurity threats, and collect, process, and analyze cybersecurity-related information that may have an impact on business and IT environments. To support customers in threat detection and

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				criticality of the bank's information or IT assets. Monitoring may be real-time (to alert on suspicious activities like brute force attacks on administrator passwords or attempts to access servers via unusual ports) or periodic (e.g., end-of-day)—based on risk levels.	analysis, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. TIX is SaaS-based and supports multiple delivery methods, including web portals, APIs, SDKs, TIP integration, and mini-programs, meeting varied customer needs. It can also integrate with customers' existing security products to enhance overall security operations and threat response efficiency. Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable.
16		5.2.3.7	Information Security Incident Handling	Banks must consider the following when handling information security incidents:	The customer shall establish procedures and processes for incident management, set up a dedicated incident response team, and record, analyze, and report security incidents. The

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
		Procedures	a. Banks must identify types of information security incidents; b. Bank employees, freelancers, and IT service provider staff must report any knowledge, discovery, or indication of potential information security incidents ; c. Banks must consider establishing a dedicated incident response team; d. Banks must establish incident reporting procedures; e. Banks must establish incident handling procedures ; f. Banks must maintain complete documentation of each information security incident; g. Banks must regularly review incident handling guidelines to ensure alignment with the bank's current IT system state; h. Banks may consider providing incentives to bank employees, freelancers, and IT service provider staff who report incidents or IT vulnerabilities at risk of exploitation— to	customer shall also regularly review the incident handling guidelines to ensure they are consistent with the bank's current status. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—Cloud Security Center (CSC). Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the efficiency of security operations. For incident management, Tencent Cloud has established incident and service request management procedures and formulated an incident management policy. This ensures that all incidents related to IT service management activities are recorded and categorized, prioritized based on impact and urgency, and escalated as needed to ensure rapid resolution and closure. These measures minimize the impact of incidents, maintain normal business operations, and enhance customer satisfaction. Regarding incident communication and notification, Tencent Cloud has developed an information security incident management standard, which includes procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				strengthen information security.	based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. In terms of customers reporting issues to Tencent Cloud or initiating contact, Tencent Cloud offers online chat and telephone support via the cloud console and official website, allowing customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates geographically redundant customer service centers, providing 24/7 support to handle customer requests, deliver round-the-clock technical assistance for cloud products, and ensure timely, high-quality service responses. Customers may also select an appropriate support plan, which can include access to dedicated support groups, a designated technical account manager, and value-added services for enhanced assistance.
N/A	5.3.1-5.3.2	Information security risk management process		Banks must measure the likelihood of information security risks for each asset and the potential impact of losses from compromised confidentiality, integrity, or availability of these assets— to determine the level of potential risk to be addressed. Internal controls must also be implemented to ensure information security controls are properly applied, adequate, and effective— in line with	Customers should regularly identify threats and vulnerabilities applicable to their IT environment, analyze and assess the risks posed by these threats and vulnerabilities, prioritize risks, develop risk mitigation measures, evaluate residual risks, and monitor the effectiveness of risk control measures. To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. • Risk Identification: Tencent Cloud conducts risk assessments regularly, identifying applicable risk scenarios from sources such as industry security incident

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				applicable policies, standards, and procedures.	reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. • Risk Assessment: Tencent Cloud evaluates asset value, the likelihood of risk scenarios, and the potential impact, then calculates the risk level. • Risk Treatment: Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items, the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored. • Risk Monitoring, Review, and Reporting: Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions.

5.6 Disaster Recovery Plan

No. regulation	Implement ation Rules	Domain	Summary of Controls	Tencent Cloud's Response
15	6.2	Policies, standards and procedures related to disaster recovery plans	(1) A Bank shall be obligated to have a Disaster Recovery Plan. (2) A Bank shall be obligated to ensure that the Disaster Recovery Plan referred to in Paragraph (1) can be implemented effectively, to maintain the Bank's operational continuity in the event of a disaster and/or disruption to the Information Technology facilities used by the Bank. (3) A Bank shall be obligated to test the Disaster Recovery Plan for all critical applications and infrastructure at least once a year, with the participation of Information Technology users. (4) A Bank shall be obligated to review the Disaster Recovery Plan at least once a year.	Customers shall formulate a comprehensive disaster recovery plan and ensure its ongoing effectiveness. Specifically, this includes: conducting tests on the disaster recovery plan for critical applications and infrastructure at least once a year based on the results of business impact analysis to verify its feasibility; and conducting a full review of the plan at least once a year to ensure it remains aligned with business requirements and the technological environment, thereby guaranteeing the ability to restore business operations quickly and effectively in the event of a disaster. To enable customers to respond rapidly and restore critical functions in the event of a disaster, multiple products provided by Tencent Cloud are equipped with high-availability features to help customers achieve high availability of their systems or services, including the following examples: • <u>Cloud Load Balancer (CLB)</u> delivers secure and efficient Layer 4 and Layer 7 traffic distribution services. It expands the external service capabilities of application systems through traffic distribution and eliminates single points of failure. CLB adopts a clustered deployment architecture and automatically removes faulty instances in a timely manner to achieve high availability. • <u>Cloud Virtual Machine (CVM)</u> features high service availability and data reliability. The Cloud Block Storage (CBS) mounted on CVM adopts a triple-replica storage strategy,

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				which ensures rapid data migration and recovery if any replica malfunctions. • <u>Cloud Object Storage (COS)</u> provides cross-architecture and cross-device redundant data storage, and offers remote disaster recovery and resource isolation capabilities for customer data to ensure data durability. • <u>TencentDB for MySQL</u> supports high data reliability and service availability, with a robust mechanism for automatic data backup and lossless recovery. • <u>Tencent Kubernetes Engine (TKE)</u> adopts a distributed service architecture to ensure automatic service failure recovery and rapid migration. Combined with distributed storage for stateful service backends, it achieves secure and highly available services and data. A variety of storage and database services provided by Tencent Cloud are equipped with backup capabilities to meet customers' diverse backup requirements. Examples are as follows: • Data stored by customers in <u>Cloud Object Storage (COS)</u> can be replicated across multiple designated regions through the cross-region replication feature, ensuring that complete data can still be retrieved and restored from redundant copies in case of accidental partial data loss. This also prevents losses caused by unavoidable disasters affecting storage in a single availability zone, achieving the effect of multi-redundancy backup and remote disaster recovery.

No.		Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules			
				- The snapshot backup feature of Cloud Block Storage (CBS) backs up data by capturing point-in-time snapshots of CBS, preventing data loss caused by tampering or accidental deletion and enabling quick rollback in the event of service failures. Cloud File Storage (CFS) offers a scheduled snapshot feature, allowing customers to flexibly configure backup policies. It is recommended that customers adopt different scheduled snapshot policies for different business scenarios. TDSQL-C for MySQL, the cloud-native database, supports two backup types: logical backup and snapshot backup. With full data backups plus subsequent binlog backups over a period of time, the entire TDSQL-C for MySQL cluster or specific databases and tables can be restored to any point in time. TencentDB for MySQL supports both automatic and manual database backup methods, and provides cross-region backup capabilities to help customers enhance their disaster recovery capabilities and improve data reliability. TencentDB for MongoDB is equipped with an automatic data backup and lossless recovery mechanism, supporting multi-node data backup. Customers can retain backup data for multiple days through this mechanism to facilitate data recovery in disaster scenarios.

Tencent Cloud regions are fully isolated from

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				each other to maximize stability and fault tolerance across regions. To ensure high data availability, each region is further divided into multiple mutually isolated availability zones. Tencent Cloud's multi-availability zone design effectively mitigates the impact of single points of failure and ensures fault isolation between availability zones, thereby guaranteeing business continuity for customers. In addition, to ensure continuous availability of customer business, Tencent Cloud has designed and implemented a business continuity management framework suitable for its own cloud computing environment, and has obtained the international standard certification of ISO/IEC 22301 for business continuity management systems. Tencent Cloud conducts business impact analysis on its cloud products and services, clarifies the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each business, and formulates differentiated response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans have been developed for cloud products and critical processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Tencent Cloud conducts regular business continuity drills and tests on cloud products in accordance with business continuity plans to verify the feasibility of such plans and protocols. In terms of personnel support, Tencent

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
15	6.3	Testing of Disaster Recovery Plans	Testing must be conducted at least once a year for all critical systems or applications (based on BIA results), covering all critical infrastructure and involving IT users. If the bank uses IT service providers for operations, testing must also involve these external parties. For fundamental changes to the bank's IT systems, applications, or infrastructure (e.g., core banking system changes), DRP testing must be conducted within 6 months of implementing the changes.	Cloud has defined personnel roles in the business recovery process and clarified the division of responsibilities during the recovery phase. For critical skills or positions, a dual-role (A/B) backup mechanism is adopted, and regular emergency drill training is conducted to ensure the rapid and effective execution of recovery procedures, supporting customers in achieving timely recovery in the event of business disruptions. Customers shall conduct regular tests on their disaster recovery plans to verify the effectiveness of such plans. For information assets managed by service providers, customers shall assess the service providers' disaster recovery capabilities and collaborate with them to conduct testing. Customers can leverage Tencent Cloud Smart Advisor (TSA) to support the planning and execution of business continuity testing. As a cloud governance platform with vertical applications across multiple IT Operations Management (ITOM) domains, this service draws on the extensive operational expertise of Tencent Cloud professionals and optimizes cloud infrastructure through multiple governance measures such as risk inspections and fault drills. Tencent Cloud Advisor is capable of providing a wide range of fault injection scenarios spanning from Infrastructure as a Service (IaaS) to Platform as a Service (PaaS), as well as drill experience templates across various industries. It covers multiple typical application scenarios including cross-availability zone disaster recovery, helping customers rapidly and efficiently reuse proven solutions based on their specific business needs and enhance system

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				availability. To ensure the continuous availability of customers' business operations, Tencent Cloud formulates differentiated response strategies and business continuity plans based on the results of business impact analysis on cloud products and services, and develops detailed disaster recovery plans for cloud products and critical processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Tencent Cloud regularly conducts drills and tests for emergency response and disaster recovery internally. Tencent Cloud performs risk assessments on the drill plans to avoid any negative impact on services due to the drills. Tencent Cloud's disaster recovery drills are usually conducted by simulating real-world, classic disaster recovery scenarios, including offensive and defensive drills and large-scale failures, to comprehensively verify the system's disaster recovery capability, response speed and recovery efficiency. Upon completion of the drills, the relevant departments are required to compile drill reports, implement rectifications based on identified improvement measures, and file and retain the reports for future reference. If the customer assesses that the disaster recovery drill requires Tencent Cloud's participation and collaboration, Tencent Cloud will respond promptly and fully cooperate. Based on the specific needs of the customer, Tencent Cloud will clearly define

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				the scenario and scope of the drill, jointly formulate a detailed drill plan and execution schedule. During the drill, Tencent Cloud will provide necessary technical support and resource guarantees, assist the customer in continuously optimizing the disaster recovery strategy and process, and jointly enhance business continuity and disaster recovery capabilities.
N/A	6.4	Maintenance of Disaster Recovery Plans and Internal Audits	Banks must update DRP to ensure alignment with internal and external conditions. These changes must be analyzed for their impact on the current DRP, and necessary improvements identified to integrate changes into the updated DRP. The revised DRP must be documented and distributed to IT units. Internal auditors must examine: a. Alignment of DRP with the bank's risk management policies; b. Whether DRP covers critical activities (based on the bank's BIA); c. Adequacy of DRP to control and mitigate risks identified in risk assessments; d. Adequacy of DRP testing procedures; e. Effectiveness of DRP	Customers should update their disaster recovery plans on a regular basis to ensure alignment with the internal and external environment of the enterprise, and conduct periodic internal audits of such plans. These audits must ensure consistency with the company's risk management policies, cover the critical activities identified in business impact analysis results, and ensure that major audit findings and audit reports are submitted in a timely manner. Tencent Cloud conducts an annual assessment of the completeness, rationality and effectiveness of its business continuity management system, and revises the system based on the assessment outcomes. Tencent Cloud also reviews its business continuity plans annually and updates them as necessary in accordance with the review results. In the event of material changes to business functions or critical resources, Tencent Cloud will review the scope of key businesses and functions as well as the inter-component dependencies, and revise the business continuity plans promptly. Tencent Cloud also engages third-party institutions on a regular basis to audit the implementation of its business continuity management practices, ensuring compliance with the requirements of the ISO 22301

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
		test implementation; f. Currency of DRP (aligned with the bank's operational developments and latest test results). Internal auditors must communicate audit results and provide recommendations to the board of directors. The board should review the audit report and plan improvements or corrections.	Business Continuity Management System. For non-conformities identified in the audits, Tencent Cloud will promptly analyze the actual and potential root causes, assess the necessity and priority of implementing corrective and preventive actions, and execute such actions upon obtaining relevant approvals. The effectiveness of the implemented corrective actions will be continuously tracked and documented.

5.7 Internal Audit

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
19	8.2-8.3 Policies, Standards and Procedures Relating to IT Audits	(1) A Bank shall be obligated to have internal audit guidelines for Information Technology use (whether operated by the Bank itself and/or by Information Technology service providers). (2) A Bank shall be obligated to review the Information Technology internal audit function at least once every three years. (3) The review referred to in Paragraph (2) shall be	Customers should establish an internal audit mechanism for information technology usage, and arrange for an independent third party to review the functions of the information technology internal audit at least once every three years. Customers should also submit the results of internal and external audits to the financial services regulator. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
		conducted by an independent external party. (4) A Bank shall be obligated to submit the following to the Financial Services Authority: a. The results of the review referred to in Paragraph (3), including improvement recommendations as part of the review report; b. The results of the Information Technology internal audit as part of the internal audit implementation report and key audit findings, in accordance with the regulatory requirements for internal audit function implementation standards.	and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. In addition, Tencent Cloud undergoes annual professional audits conducted by independent third parties both at home and abroad. By providing attestation-based System and Organization Controls (SOC) reports, we disclose the latest internal control status of our service organization to cloud user institutions, independent auditors, regulatory authorities, corporate shareholders and other relevant stakeholders. To ensure that Tencent Cloud's information technology policies, procedures, processes, and control measures meet the requirements of Indonesian financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Indonesian financial industry conducted by an independent third party. Customers can independently download the latest report from the Tencent Cloud Compliance Document Center. Tencent Cloud will actively comply with customers' outsourcing management requirements, and fully respond to and cooperate with audit or assessment activities initiated by customers.

5.8 Engagement of Information Technology Service Providers

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
20	9.2 Policies, Standards and Procedures for the	(1) A Bank shall operate Information Technology. (2) The operation of Information Technology	If customers' information technology operations are performed by information technology service providers, the customers shall establish processes for engaging

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			Engagement of IT Service Providers	referred to in Paragraph (1) may be conducted by the Bank itself and/or by Information Technology service providers. (3) If the Bank's Information Technology operation is conducted by an Information Technology service provider (referred to in Paragraph (2)), the Bank shall be obligated to: a. Be responsible for the implementation of risk management; b. Maintain an Information Technology unit; c. Have a highest-ranking official leading the Information Technology unit; d. Be able to oversee the Bank's activities operated by the service provider; e. Select the Information Technology service provider based on cost-benefit analysis, with the participation of the Bank's Information Technology unit; f. Regularly monitor and evaluate the reliability of the Information Technology service	external IT service providers. These processes shall include submitting requirements, issuing requests for proposals to IT service providers, conducting due diligence, entering into contractual agreements with IT service providers, and specifying special terms and conditions, among others. In addition, customers shall ensure that IT service providers provide access to data and information when required by internal and external auditors and regulatory authorities. In terms of due diligence, Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. The following is an overview of Tencent Cloud's practices as a cloud service provider in responding to due diligence requirements across various aspects: • Reputation and Industry Experience As the cloud computing brand of Tencent—a leading enterprise in China's internet industry—Tencent Cloud has obtained a number of professional certifications from industry authorities. It offers comprehensive cloud computing solutions and has provided reliable cloud services to a vast array of enterprise and government customers, earning recognition from customers across diverse industries worldwide. • Professional Personnel Tencent Cloud has established a Security Technology Committee, specialized security teams across various functions and domains, and assembled a team of seasoned industry experts. We are committed to delivering

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			provider (covering performance, service provider reputation, and service continuity); g. Provide access to internal auditors, external auditors, and the Financial Services Authority to obtain data and information whenever needed; h. Provide the Financial Services Authority with timely access to the Database (for both current and historical data); i. Ensure the Information Technology service provider: 1.Has reliable experts with academic and/or professional certification relevant to Information Technology operation needs; 2.Implements adequate Information Technology control principles (evidenced by audit results from an independent party); 3.Provides access to the Bank's internal auditors, external auditors appointed by the Bank, the Financial Services Authority, and/or other	secure, reliable, professional and compliant products and services to our customers. Technical strengths: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products, ensuring reliable and continuous service for customers. Operational Capability and Scale Tencent Cloud ranks among the industry leaders in terms of operational capability and scale. Our data centers are located across multiple regions globally, covering mainland China, the Asia-Pacific, North America and Europe. We have partnered with over 11,000 organizations and delivered more than 400 industry-specific solutions to enterprise customers spanning over 30 sectors. Financial stability: Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant.

No.	regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				authorized parties (in accordance with applicable laws and regulations) to conduct inspections and obtain necessary data and information timely whenever needed;	• Compatibility with the Customer's Corporate Culture and Future Development Strategy Tencent Cloud can customize solutions to meet customers' specific needs, with flexible adaptation to different corporate cultures and strategic objectives.
				4.Consents to inspections by the Financial Services Authority and/or other legally authorized parties of the provided services;	• Familiarity with the Banking Industry Tencent Cloud has tailored a wide range of solutions for numerous financial institutions, providing them with a comprehensive "technology platform + security experts" service solution. This helps them effectively address security challenges, enhance security protection capabilities, and meet security compliance requirements.
				5.(As an affiliated party) Maintains the security of all information, including Bank secrets and customer personal data;	• Capability to Keep Pace with Market Innovation Tencent Cloud actively tracks market trends and technological advancements, and continuously launches innovative products and services to maintain its leading market position and meet customers' latest requirements.
				6.Only sub-contracts part of its activities with the Bank's written consent;	
				7.Reports to the Bank any critical incidents that may cause significant financial losses and/or disrupt the Bank's operational continuity;	In terms of signing contractual agreements with customers, Tencent Cloud makes available a suite of legal documents on its official international website, including the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings provided by Tencent Cloud, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, as well as service terms and scenarios for agreement termination. Customers may also opt to sign offline agreements with
				8.Submits the results of independent auditor audits of Information Technology operations (for Data Centers, Disaster Recovery Centers, and/or Information Technology-Based Transaction Processing) to the Financial Services Authority through the	

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			relevant Bank;	Tencent Cloud to negotiate and finalize the specific terms and detailed provisions thereof.
			9.Provides a tested and adequate Disaster Recovery Plan;	Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console.
			10.Agrees to the possibility of early termination of the contract;	
			11.Meets the service level specified in the service level agreement between the Bank and the Information Technology service provider.	
			(4) The Bank's use of an Information Technology service provider (referred to in Paragraph (3)) shall be based on a written contract. The contract shall include at least the Information Technology service provider's commitment to implement the requirements referred to in Paragraph (3) Sub-point (i).	For subcontracting scenarios, the agreements also include clauses governing prior consent for subcontracting, notification requirements prior to adding or replacing subcontractors, and data protection obligations. Without the customer's prior written consent, Tencent Cloud shall not subcontract any processing operations performed on behalf of the customer pursuant to the contract or agreement. In the event of any intended changes involving the addition or replacement of subcontractors, Tencent Cloud will notify the customer via email or other designated channels. Regarding customers' continuous monitoring and evaluation of Tencent Cloud, in terms of customer audits and regulatory reviews, Tencent Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. In addition, Tencent Cloud's security team continuously monitors and assesses internal

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				security risks to ensure the effectiveness and reliability of our information security management system.. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. In addition, Tencent Cloud undergoes annual professional audits conducted by independent third parties both at home and abroad. By providing attestation-based System and Organization Controls (SOC) reports, we disclose the latest internal control status of our service organization to cloud user institutions, independent auditors, regulatory authorities, corporate shareholders and other relevant stakeholders. To ensure that Tencent Cloud's information technology policies, procedures, processes, and control measures meet the requirements of Indonesian financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Indonesian financial industry conducted by an independent third party. Customers can independently download the latest report from the Tencent Cloud Compliance Document Center. If customers need to terminate or discontinue cloud services, they may back up and migrate their cloud-based data and production environments at any time. Tencent Cloud's products support data backup and migration in universal standard formats. As such, customers can leverage the same transmission methods and protocols used during cloud onboarding, or adopt network service products such as Direct Connect (DC) and VPN Connection, to ensure the security and reliability of data

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				during termination of cloud service engagement. Upon termination of the customer's services, Tencent Cloud will adhere to strict data erasure methods, all customer data—including copies and backups—will be permanently deleted upon the expiration of the retention period, with no possibility of recovery. When the media used to provide Tencent Cloud services malfunctions and requires replacement or reaches the end of its service life and needs to be decommissioned, Tencent Cloud will promptly carry out complete physical destruction in accordance with rigorous procedures. If customers are required to provide regulatory authorities with access to electronic systems or electronic data, they may utilize Tencent Cloud's Cloud Object Storage (COS). COS is a distributed storage service designed for storing massive volumes of files, enabling users to store and retrieve data anytime via the internet. Users can manage the access permissions of buckets and objects; upon receiving an access request for a specific resource, COS will verify the corresponding Access Control List (ACL) to confirm whether the requester holds the required permissions. After creating a Tencent Cloud sub-account, users can assign permissions to the sub-account through access policies. If it is necessary to open resources to non-Tencent Cloud users, this can be achieved by configuring public read permissions for the relevant resources (buckets, objects, directories). Through the aforementioned features, customers can provide electronic data to regulatory authorities for review as required.

No. regulation	Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
				Furthermore, Tencent Cloud is committed to protecting the data security of customers worldwide and complies with the applicable laws and regulations of the countries or regions where we operate. Customer data is classified as high-security-level data within Tencent Cloud's infrastructure. Customers retain sole ownership and control over their own data content. Unless such access is necessary for service provision or troubleshooting with the customer's explicit authorization, or required by national laws and regulations such as investigations into criminal matters by national or local government authorities, no internal Tencent Cloud employee will proactively access any customer data.
N/A	9.3.4	Additional Risk Controls	Even if banks and IT service providers deploy advanced systems, non-compliance incidents (such as human error, process vulnerabilities, and employee theft) may still occur. Banks shall implement security controls to mitigate such risks, including the following measures: a. Requiring IT service providers to conduct background checks on their employees; b. Clearly defining the providers' obligations for the security control of IT facilities, data and information in the agreement;	Customers should require IT service providers to conduct background checks on their employees, clearly define the IT providers' information security and data security obligations and liabilities in the agreement, and ensure that security costs are commensurate with the required security level. Tencent Cloud signs confidentiality agreements with its internal employees, which cover the signatories' confidentiality obligations and responsibilities, as well as the potential penalties for breaching the confidentiality clauses. Background checks are also required for contracted employees prior to their employment, who shall be bound by the confidentiality requirements stipulated in the agreement signed between Tencent Cloud and the contracting agencies. The confidentiality requirements between Tencent Cloud and its employees and third parties are reviewed and updated by the legal

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			c. Ensuring that the providers understand and meet the security requirements of the bank based on the confidentiality sensitivity of data; d. Ensuring that security costs are commensurate with the required security level and aligned with the bank's risk tolerance.	department as necessary. In terms of contracts and agreements, Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure requirements. Customers can also choose to sign a customized agreement with Tencent Cloud to negotiate and modify specific terms and rules in the agreement.
N/A	9.4	Monitoring and Oversight of IT Service Providers	Banks should formulate a monitoring plan to ensure that IT service providers perform their obligations in accordance with the agreement. Banks should conduct reviews both prior to and after the commencement of cooperation to ensure the effective implementation of risk management policies, standards and procedures. In addition, banks shall conduct periodic reviews on performance and Service Level Agreement (SLA) compliance, and compile review reports. Monitoring activities shall include the	Customers shall conduct reviews both prior to and after commencing cooperation with IT service providers, and perform periodic reviews on performance and SLA compliance. To support customers outsourcing supervision requirements, Tencent Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. In addition, The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules	assessment of review reports submitted by the providers. Banks should conduct regular audits on IT service providers (either by internal or external auditors), where the scope of such audits shall be consistent with the service scope specified in the agreement.	undergoes annual independent professional audits by domestic and international third parties. Through System and Organization Controls (SOC) reports, Tencent Cloud provides assurance to cloud customers, independent auditors, regulators, shareholders, and other stakeholders regarding its latest internal control status. Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console.

5.9 Reporting

No.	Domain	Summary of Controls	Tencent Cloud's Response
regulation	Implementation Rules		
31	N/A	Incidental Reports (1) A Bank shall be obligated to report critical incidents, misuse, and/or crimes in the operation of Information Technology that may and/or have caused significant financial losses and/or disrupted the Bank's operational continuity. (2) The report referred to in Paragraph (1) shall be	In the event of any major incidents, misuse or criminal activities occurring in information technology operations, customers shall immediately report such matters to the financial regulatory authority via email or telephone, and submit a written report within a maximum of 7 working days. To support customers in meeting regulatory requirements, Regarding incident communication and notification , Tencent Cloud has developed an information security incident management standard, which includes procedures for incident response,

No.	regulation Implementation Rules	Domain	Summary of Controls	Tencent Cloud's Response
			submitted immediately to the Financial Services Authority via email or telephone, followed by a written report within a maximum of 7 (seven) working days after the Bank becomes aware of the critical incident, misuse, and/or crime.	escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. Regarding customers reporting issues to or proactively contacting Tencent Cloud, Tencent Cloud offers a ticket service through the console on its official website, enabling customers to report faults, incidents, problems and complaints related to security, availability and confidentiality. In addition, Tencent Cloud offers online chat and telephone support via the cloud console and official website, allowing customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates geographically redundant customer service centers, providing 24/7 support to handle customer requests, deliver round-the-clock technical assistance for cloud products, and ensure timely, high-quality service responses. Customers may also select an appropriate support plan, which can include access to dedicated support groups, a designated technical account manager, and value-added services for enhanced assistance.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Implementation of Information Technology by Commercial Banks and Non-Bank Financial Institutions

The application of information technology has increased the risk exposure faced by financial institutions. To mitigate such risks, financial institutions must strengthen information technology governance and optimize resource allocation, thereby creating additional value for their businesses. In response to this need, the Indonesian Financial Services Authority (OJK) formulated and issued Regulation No. 04/POJK.05/2021 on the [Implementation of Risk Management in the Use of Information Technology by Non-Bank Financial Institutions](#), aiming to regulate and refine the risk management practices of non-bank financial institutions¹ (LJKNB) in their application of information technology.

Furthermore, to dynamically align with the evolving standards of information technology application and development, the Indonesian Financial Services Authority further revised Regulation No. 38/POJK.03/2016 on the Implementation of Risk Management in the Use of Information Technology by Commercial Banks and its amendments in 2022, and promulgated [Regulation No. 11/POJK.03/2022 on Organization of Information Technology Implementation by Commercial Banks](#).

The provisions of these two regulations primarily focus on information technology governance, IT organizational structure, the application of IT operational risk management, the engagement of IT service providers, electronic system deployment, and personal data protection, with their content being highly similar. Therefore, in this chapter, Tencent Cloud will extract, integrate and summarize the control requirements relevant to cloud service providers as set forth in Regulation No. 04/POJK.05/2021 and Regulation No. 11/POJK.03/2022, and elaborate on how Tencent Cloud, as a cloud service provider, can assist commercial banks in complying with these requirements.

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank Financial Service Institutions (NBFIs)	Commercial Banks			
9	N/A	Adequacy of Policies and Procedures for Information Technology Usage	(1) NBFIs shall have policies and procedures for the use of Information Technology. (2) NBFIs shall implement the policies and procedures for the use of Information Technology (referred to in paragraph (1)) consistently and continuously. (3) The policies and procedures for the use of	Customers should formulate policies, standards, and processes for the use of information technology, regularly review and update these policies and processes, and set tolerable risk limits to ensure the optimal operation of information technology-related aspects. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy,

¹ Nonbank Financial Service Institutions (NBFIs) shall mean institutions engaged in activities in the insurance, pension fund, financing institution, and other financial service institution sectors.

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			Information Technology shall include at least the following aspects: a. Management; b. Development and procurement; c. Information Technology operations; d. Communication networks; e. Information security; f. Disaster Recovery Plans; g. The use of Information Technology service providers; and h. Electronic Financial Services (for NBFIs that operate Electronic Financial Services). (4) NBFIs shall set tolerable risk limits to ensure that the Information Technology-related aspects referred to in paragraph (3) can operate optimally. (5) NBFIs shall review and update the policies and procedures referred to in paragraph (2) periodically. (6) NBFIs shall specify the timeframe for reviewing and updating the policies and procedures referred to in paragraph (5) in a written	security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards.

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			policy.	
11	15	Risk Management	(1) Banks shall implement effective risk management in IT operations. (2) The implementation of risk management referred to in paragraph (1) must be integrated into every stage of IT operations. (3) In implementing the risk management referred to in paragraph (1), Banks shall conduct at least the following processes: a. risk identification; b. risk measurement; c. risk monitoring; and d. risk control. (4) Banks shall ensure the adequacy of the risk management information system for IT operations.	To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. • Risk Identification: Tencent Cloud conducts risk assessments regularly, identifying applicable risk scenarios from sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. • Risk Assessment: Tencent Cloud evaluates asset value, the likelihood of risk scenarios, and the potential impact, then calculates the risk level. • Risk Treatment: Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items,

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored. Risk Monitoring, Review, and Reporting: Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. In addition, Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions.
12	N/A	Information Technology Development	(1) When developing Information Technology, NBFIs shall implement control measures to produce a system that supports: a. the achievement of the NBFIs' objectives; and b. the protection of data confidentiality and integrity. (2) The control measures	When customers carry out information technology development and procurement, they should formulate and implement information technology development and procurement processes and plans, conduct project management, carry out sufficient testing, and retain process documents. In addition, customers should also establish an application system change management mechanism to ensure that information technology systems can be

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			referred to in paragraph (1) shall cover at least:	fully traced back. If the software used by the customer is developed by a third party and the source code is not provided, the customer needs to evaluate the necessity of signing a written escrow agreement with the third party.
			a. establishing and implementing consistent methodologies and procedures for the development and procurement of Information Technology;	To support customers in R&D management, Tencent Cloud provides Cloud Native Build (CNB) developer tools. CNB is based on the Docker ecosystem, abstracting environments, caches, and plugins, and uses declarative syntax to help developers build software more efficiently. CNB offers a complete developer toolchain with capabilities such as code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and custom task sets, effectively enabling end-to-end R&D process support and agile development management from requirements to deployment.
			b. implementing project management in system development and procurement;	
			c. conducting adequate testing during the development and procurement of a system, including joint testing with user units, to ensure the system's accuracy, functionality in meeting user needs, and compatibility with other systems;	
			d. documenting the development, procurement, and maintenance of Information Technology systems;	Tencent Cloud, as a cloud service provider, on its international portal, Tencent Cloud provides online legal documents such as the Terms of Service , Service Level Agreement (SLA) , and Data Processing and Security Agreement . These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both
			e. having change management for Information Technology systems;	
			f. ensuring that the NBFI's Information Technology system can restore	

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			information completely; and g. ensuring the execution of written agreements for software (if the software affects the NBFI's operational continuity and is developed by a third party). f. Ensure that the bank's information technology systems support the complete traceability of information; g. Assess the necessity of signing a written escrow agreement — if software is developed by a third party, the source code is not provided to the bank, and the software is critical to the bank's operational continuity, such an agreement shall be signed.	customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. To support customers in meeting regulatory requirements, in terms of secure system development, Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls throughout the product lifecycle. Key security measures include: • Security Training: Developers receive secure coding training and are required to follow secure coding guidelines. • Requirements Analysis: Engage in discussions on business content, workflows, and technical frameworks to identify optimal security integration points. • System Design: Perform threat modeling and security assessments of the chosen architecture. • System Development: Provide

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				Tencent-designed secure development components and enforce secure coding practices. • Security Validation: Conduct code security checks, asset scans, web vulnerability scans, manual security assessments, penetration testing, and code audits to identify vulnerabilities. • Release: Systems are deployed to production Only after all high-risk issues have been fixed to prevent vulnerabilities from entering the live environment. In terms of system testing, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams. For third-party product usage, Tencent Cloud has defined software

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies. In terms of change management, Tencent Cloud has established a set of management standards for product and configuration changes, all types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment.
17	16	Information Security	(1) Banks and Financial Institutions shall ensure the effective and efficient implementation of	Customers shall implement information security management based on the results of information asset risk assessments, covering technical, human

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			information security. (2) The information security referred to in paragraph (1) shall cover human resources, processes, technology, and physical or environmental aspects throughout IT operations. (3) The implementation of information security referred to in paragraph (1) shall be based on the results of risk assessments of the information owned by the Bank and Financial Institutions.	resource, and procedural aspects of information technology usage, to maintain the confidentiality, integrity, and availability of information. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. For further details related to human resources, processes, technologies, and

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				physical or environmental aspects, please refer to " 5.5 Information Security " in this guideline.
				Customers shall provide a communication network that complies with the principles of confidentiality, integrity, and availability.
				Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures. Similarly, Tencent Cloud's compute nodes adopt redundancy, and any faulty node is automatically removed by the scheduler in real time, ensuring service continuity for Customer workloads.
14	17	Communication Networks	Bank and Financial Institutions shall ensure that the communication networks provided by the Bank meet the principles of confidentiality, integrity, and availability.	In terms of network communication security, all communications on the Tencent Cloud Console are encrypted using the HTTPS protocol. Tencent Cloud's cloud API interfaces provide HTTPS encryption, signature verification, and status monitoring to ensure port-level communication security for customer operations. Direct Connect (DC) offers dedicated, high-security, high-bandwidth network connections, enabling customers to use exclusive network links and reduce data leakage risks. Customers can also use Cloud Connect Network (CCN) to establish secure private interconnections between VPCs or between VPCs and on-premises data

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank Financial Service Institutions (NBFIs)	Commercial Banks			
16	18	Business Continuity	(1) Banks and Financial Institutions shall have a Business Continuity Plan (BCP). (2) Banks and Financial Institutions shall ensure that the Business Continuity Plan referred to in paragraph (1) is implementable, so that the Bank's operational continuity remains uninterrupted in the event of a disaster and/or disruption to the IT facilities used by the Bank. (3) Banks and Financial Institutions shall conduct tests of the Business Continuity Plan for all critical applications and infrastructure (based on business impact analysis results) at least once a year, with the participation of IT users. (4) Banks and Financial Institutions shall review the Business Continuity Plan at least once a year.	centers (IDCs). For further details related to communication networks, please refer to “5.4 Information Technology Communication Networks” in this guideline. Customers shall formulate a disaster recovery plan, test the disaster recovery plan for critical applications and infrastructure at least once a year based on the results of business impact analysis, and ensure its effective implementation. Customers shall also review the disaster recovery plan at least once a year. Tencent Cloud builds or leases data centers worldwide in compliance with international standards and local security requirements, offering customers multi-region and multi-zone options to meet disaster recovery and service level objectives. Tencent Cloud's compute, network, storage, database, container, and middleware services provide highly available architectures and support customer-defined backup strategies to meet diverse backup needs. In addition, to ensure the continuous availability of customers' businesses, Tencent Cloud has designed and implemented a business continuity management framework suitable for its own cloud computing environment, and has obtained the international standard certification of ISO/IEC 22301

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks			
			(5) Banks and financial institutions shall specify the time limits for the tests mentioned in Clause (3) and the reviews mentioned in Clause (4) in their written policies.	Business Continuity Management System. Tencent Cloud conducts business impact analysis on its cloud products and services, clarifies the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each business, formulates differentiated response strategies and business continuity plans based on the analysis results, and develops detailed disaster recovery plans for cloud products. Tencent Cloud conducts regular business continuity drills and tests on cloud products in accordance with business continuity plans to verify the feasibility of such plans and protocols. Tencent Cloud reviews its business continuity plans annually and updates them as necessary based on the review results. In the event of material changes to business functions or critical resources, Tencent Cloud will review the scope of key businesses and functions as well as the inter-component dependencies, and revise the business continuity plans promptly. For further details related to business continuity plans, please refer to “5.6 Disaster Recovery Plan” in this guideline.
N/A	21	Cyber Resilience	(1) Banks shall maintain cyber resilience. (2) To maintain the cyber resilience referred to in paragraph (1), Banks shall conduct at least the	Customers shall establish processes for asset protection, threat and vulnerability identification, cyber incident detection, and response and recovery, to ensure the risk resilience of information technology.

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			following processes: a. identification of assets, threats, and vulnerabilities; b. asset protection; c. cyber incident detection; and d. cyber incident response and recovery. (3) Banks shall ensure that the processes for maintaining cyber resilience referred to in paragraph (2) are supported by an adequate cyber resilience information system.	To assist customers in comprehensive information asset management, Tencent Cloud provides <u>Cloud Workload Protection Platform (CWPP)</u>, which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, <u>Cloud Security Center (CSC)</u>, for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such as cloud configuration risks, vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. To support customers in meeting regulatory requirements, Tencent Cloud has formulated information asset management specifications and full-lifecycle management processes, which conduct classified and hierarchical management and protection of assets such as electronic data, hardware and

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				their virtual devices, infrastructure, application systems, and software. Tencent Cloud manages hardware devices and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, etc. This ensures the stable operation of the underlying system of the cloud platform and provides reliable support for business systems. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—Cloud Security Center (CSC). Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the efficiency of security operations. Tencent Cloud has established incident and service request management procedures and formulated an incident management policy. This ensures that all incidents related to IT service management activities are recorded and categorized, prioritized based on impact and urgency, and escalated as needed to ensure rapid resolution and closure. These measures minimize the impact of

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				incidents, maintain normal business operations, and enhance customer satisfaction.
				To support customers in threat detection and analysis, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy.
N/A	23	Cyber Security Testing	Banks shall conduct cyber security testing based on: a. vulnerability analysis; and b. scenarios.	Customers shall conduct periodic vulnerability-based analyses and submit the test results to the financial services authority. In addition, customers shall perform scenario-based
N/A	24	Cyber Security Testing based on Vulnerability Analysis	(1) Cyber security testing based on vulnerability analysis shall be conducted periodically. (2) Banks shall submit the results of the cyber security	cybersecurity tests at least once a year, and submit a cybersecurity test result report to the financial services authority within a maximum of ten working days upon completion of the tests. In terms of penetration testing, Tencent

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			testing based on vulnerability analysis (referred to in paragraph (1)) to the Financial Services Authority as part of the report on the Bank's latest IT operation status.	Cloud provides customers with Penetration Testing Service (PTS) . By fully simulating attack techniques and vulnerability discovery methods that may be employed by hackers, PTS adopts controlled and non-destructive approaches to conduct in-depth security detection on target systems, identify vulnerabilities existing in targets and network devices, and provide security hardening recommendations to help customers enhance system security and support verification after vulnerability remediation. For vulnerability scanning, customers can opt for Vulnerability Scanning Service (VSS) to detect enterprise network assets and identify their risks. Leveraging Tencent's years of accumulated security experience and threat intelligence, VSS has established a comprehensive and robust vulnerability rule database, and is equipped with professional and efficient 0Day/1Day/NDay vulnerability detection capabilities. It can perform regular security scans, continuous risk alerts, and vulnerability detection on the availability, security, and compliance of customer assets, provide customers with professional remediation recommendations, and mitigate security risks. VSS also supports integration with cloud products such as host security and web application firewalls, forming a closed loop from risk monitoring to risk disposal.
N/A	25	Cyber Security Testing based on Scenarios	(1) Cyber security testing based on scenarios (referred to in Article 23 letter b) shall be conducted at least once a year. (2) The cyber security testing based on scenarios referred to in paragraph (1) shall cover at least: a. determination of testing objectives, scope, and scenarios; b. implementation of the testing; c. evaluation of testing results; and d. assessment of the effectiveness of the Bank's mitigation efforts, response, and recovery actions against cyber attacks. (3) Banks shall submit the report on the results of the scenario-based cyber security testing (referred to in paragraph (1)) to the Financial Services Authority no later than 10 working	

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank Financial Service Institutions (NBFIs)	Commercial Banks			
			days after the completion of the cyber security testing. (4) The report on the results of the cyber security testing referred to in paragraph (3) shall cover at least: a. a summary of the testing implementation; b. lessons learned or observations from the testing results; and c. plans or improvements that have been made.	To assist customers in complying with regulatory requirements, Tencent Cloud regularly generates scanning tasks through its vulnerability scanning system to conduct vulnerability scans on assets in the cloud environment, and performs analysis, classification, and remediation of detected vulnerabilities. In addition, Tencent Cloud conducts periodic full-link large-scale penetration tests to proactively identify and remediate potential system security risks at an early stage, and flexibly carries out targeted penetration tests prior to the launch of new products or in the event of material changes. Penetration test results are notified to the relevant responsible departments via security tickets, and the responsible departments shall promptly carry out vulnerability remediation or implement other compensating control measures to ensure that exploitable vulnerabilities identified in penetration tests are properly addressed. Furthermore, Tencent Cloud conducts regular red team-blue team exercises to simulate real-world cyberattack defense drills. Tencent Cloud has also established an external vulnerability feedback platform and launched a bug bounty program, inviting industry security experts to help identify system security vulnerabilities and risks from a hacker's perspective, so as to remediate security issues in a timely manner and maintain the security of the Tencent

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank Financial Service Institutions (NBFIs)	Commercial Banks			
				Cloud ecosystem.
				Meanwhile, Tencent Cloud has formulated a cybersecurity emergency response plan, covering various cybersecurity emergency scenarios such as cyberattacks, malicious programs, data security incidents, equipment and facility failures, and catastrophic events. Based on improving the emergency response plan system, supported by building an emergency response team, and focusing on standardizing emergency response processes, Tencent Cloud further enhances the capabilities of monitoring, early warning, notification, and disposal, so as to prevent and reduce the adverse impacts of cybersecurity incidents on Tencent Cloud.
21	30	Use of IT Service Providers	(1) Banks and financial institutions shall operate information technology systems. (2) The information technology operations referred to in Clause (1) may be performed by the banks and financial institutions themselves and/or by information technology service providers. (3) Where the information technology operations of banks and financial institutions are performed by the information technology	If customers' information technology operations are performed by information technology service providers, the customers shall establish processes for engaging external IT service providers. These processes shall include submitting requirements, issuing requests for proposals to IT service providers, conducting due diligence, entering into contractual agreements with IT service providers, and specifying special terms and conditions, among others. In addition, customers shall ensure that IT service providers provide access to data and information when required by internal and external auditors and regulatory authorities

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			service providers referred to in Clause (2), the banks and financial institutions shall be obligated to: - Assume responsibility for the implementation of risk management; - Establish an information technology department; - Have the information technology department led by a senior-level official; - Be able to supervise the activities of the banks and financial institutions that are operated by the service providers; - Select information technology service providers based on cost-benefit analysis, with the participation of the banks' and financial institutions' information technology departments; - Conduct regular monitoring and evaluation of the reliability of information technology service providers, including their performance, reputation and service continuity; - Provide access privileges to internal auditors, external	In terms of due diligence, Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. In terms of signing contractual agreements with customers, Tencent Cloud makes available a suite of legal documents on its official international website, including the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings provided by Tencent Cloud, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, as well as service terms and scenarios for agreement termination. Customers may also opt to sign offline agreements with Tencent Cloud to negotiate and finalize the specific terms and detailed provisions thereof. Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			auditors and the financial services regulator to enable them to obtain data and information when necessary;	monitors service performance and availability and provides real-time monitoring through the management console.
			h. Promptly provide database access privileges to the financial services regulator, covering both current and historical data;	For subcontracting scenarios , the agreements also include clauses governing prior consent for subcontracting, notification requirements prior to adding or replacing subcontractors, and data protection obligations. Without the customer's prior written consent, Tencent Cloud shall not subcontract any processing operations performed on behalf of the customer pursuant to the contract or agreement. In the event of any intended changes involving the addition or replacement of subcontractors, Tencent Cloud will notify the customer via email or other designated channels.
			i. Ensure that the information technology service providers:	
			1. Have reliable professional personnel who hold academic and/or professional certifications relevant to the requirements of information technology operations;	
			2. Implement robust information technology control principles, supported by audit results from independent third parties;	Regarding customers' continuous monitoring and evaluation of Tencent Cloud , in terms of customer audits and regulatory reviews, Tencent Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities.
			3. Provide access privileges to the internal auditors of the banks and financial institutions, the external auditors appointed by the banks and financial institutions, the financial services regulator and/or other parties authorized under applicable laws and regulations, to facilitate their	If customers need to terminate or discontinue cloud services , they may back up and migrate their cloud-based data and production environments at any time. Tencent Cloud's products support data backup and migration in

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			timely inspections and access to required data and information when necessary;	universal standard formats. As such, customers can leverage the same transmission methods and protocols used during cloud onboarding, or adopt network service products such as Direct Connect (DC) and VPN Connection , to ensure the security and reliability of data during termination of cloud service engagement.
			4.Consent to inspections of the services they provide conducted by the financial services regulator and/or other legally authorized authorities;	Upon termination of the customer's services, Tencent Cloud will adhere to strict data erasure methods, all customer data—including copies and backups—will be permanently deleted upon the expiration of the retention period, with no possibility of recovery.
			5.(When acting as related parties) Maintain the security of all information, including the confidential information of the banks and financial institutions as well as the personal data of customers;	For further details related to the engagement of information technology service providers, please refer to " 5.8 Engagement of Information Technology Service Providers " in this guideline.
			6.Only subcontract part of the activities with the prior written consent of the banks and financial institutions;	
			7.Report all major incidents that may lead to material financial losses and/or disrupt the operational continuity of the banks to the banks and financial institutions;	
			8.Submit the audit results of independent auditors on information technology operations (covering data centers, disaster recovery centers and/or information technology-based	

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			transaction processing) to the financial services regulator through the relevant banks and financial institutions; 9. Provide tested and adequate disaster recovery plans; 10. Consent to the possibility of early termination of the contract; 11. Meet the service levels agreed upon between the banks and financial institutions and the information technology service providers in the service level agreement. (4) The engagement of information technology service providers referred to in Clause (3) by banks and financial institutions shall be based on a written contract, which shall at a minimum include the information technology service providers' commitment to fulfilling the requirements set forth in Item (i) of Clause (3).	
22	N/A	Data Backup	(1) NBFIs with total assets of up to Rp500,000,000,000.00 (five hundred billion rupiahs) shall periodically back up	Customers shall regularly back up activity data processed through information technology. Those with assets exceeding 50 billion Indonesian rupiah shall maintain a data center and

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			data of activities processed using Information Technology. (2) NBFIs with total assets exceeding Rp500,000,000,000.00 (five hundred billion rupiahs) but not exceeding Rp1,000,000,000,000.00 (one trillion rupiahs) shall: a. have a Data Center; and b. periodically back up data of activities processed using Information Technology. (3) NBFIs shall specify the timeframe for backing up data of activities processed using Information Technology (referred to in paragraphs (1) and (2)) in a written policy. (4) NBFIs that: a. have total assets exceeding Rp1,000,000,000,000.00 (one trillion rupiahs); and/or b. conduct the majority of their business operations using Information Technology; shall have both a Data Center and a Disaster Recovery Center.	perform regular data backups. Non-bank financial institutions with assets exceeding 100 billion Indonesian rupiah must maintain both a data center and a disaster recovery center. Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options and strictly complies with applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Customers may flexibly deploy data and systems across different regions or availability zones based on business needs and data security requirements. Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia. A variety of storage and database services provided by Tencent Cloud are equipped with backup capabilities to meet customers' diverse backup requirements. Examples are as follows: Data stored by customers in <u>Cloud Object Storage (COS)</u> can be replicated across multiple designated regions through the

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				cross-region replication feature, ensuring that complete data can still be retrieved and restored from redundant copies in case of accidental partial data loss. This also prevents losses caused by unavoidable disasters affecting storage in a single availability zone, achieving the effect of multi-redundancy backup and remote disaster recovery. • The snapshot backup feature of Cloud Block Storage (CBS) backs up data by capturing point-in-time snapshots of CBS, preventing data loss caused by tampering or accidental deletion and enabling quick rollback in the event of service failures. • Cloud File Storage (CFS) offers a scheduled snapshot feature, allowing customers to flexibly configure backup policies. It is recommended that customers adopt different scheduled snapshot policies for different business scenarios. • TDSQL-C for MySQL, the cloud-native database, supports two backup types: logical backup and snapshot backup. With full data backups plus subsequent binlog backups over a period of time, the entire TDSQL-C for MySQL cluster or specific databases and tables can be

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				restored to any point in time.
				• <u>TencentDB for MySQL</u> supports both automatic and manual database backup methods, and provides cross-region backup capabilities to help customers enhance their disaster recovery capabilities and improve data reliability. • <u>TencentDB for MongoDB</u> is equipped with an automatic data backup and lossless recovery mechanism, supporting multi-node data backup. Customers can retain backup data for multiple days through this mechanism to facilitate data recovery in disaster scenarios.
23	35	Electronic System Deployment	(1) Banks shall place their Electronic Systems in Data Centers and Disaster Recovery Centers within the territory of Indonesia. Non-bank financial institutions that operate a data center and/or disaster recovery center shall deploy their electronic systems within the territory of Indonesia at such facilities. (2) Banks may place their Electronic Systems in Data Centers and/or Disaster Recovery Centers outside the territory of Indonesia, provided that they obtain	Customers shall host their electronic systems at data centers and disaster recovery centers located within Indonesia. If a customer chooses to host electronic systems at data centers outside Indonesia, it shall submit legal documents including national risk assessments, statements and cooperation agreements to obtain approval from the financial services regulator. Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options and strictly complies with

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			approval from the Financial Services Authority. Non-bank financial institutions that meet the requirements set forth in Clause 1 are prohibited from deploying electronic systems at data centers and/or disaster recovery centers located outside Indonesia, unless prior approval has been obtained from the financial services regulator.	applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Customers may flexibly deploy data and systems across different regions or availability zones based on business needs and data security requirements. Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia.
24	37	Continuity of Data Centers and Disaster Recovery Centers	Banks and Financial Institutions shall ensure that the Data Centers and Disaster Recovery Centers guarantee the continuity of the Bank's and Financial Institutions business operations.	Customers should formulate policies, standards, and procedures related to data center operational activities, implement physical access control for data centers, and protect the physical environment security of data centers to ensure that data centers and disaster recovery centers can guarantee the continuous operation of business. To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, organized by regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. As a cloud service provider, Tencent Cloud is committed to delivering secure, stable, continuous, and reliable physical infrastructure for customers. Currently, Tencent Cloud operates three

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				leased data centers in the Indonesia region. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. Customers can flexibly deploy data and systems across different regions or availability zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures. Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point device failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts annual on-site audits to verify that data

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures. For more information on the management of the physical environment of data centers, access control management, security and monitoring, as well as physical and environmental incidents, please refer to “5.3 Information Technology Operation Activities” clause "22\3.2.1 Policies related to data centers".
N/A	43	Data Management	(1) Banks shall manage data effectively in their data processing to support the achievement of the Bank's business objectives. (2) The effective data management referred to in paragraph (1) shall take into account at least: a. data ownership and stewardship; b. data quality; c. data management systems; and d. supporting resources for data management.	When conducting data processing activities, customers shall implement effective data governance, clarify data ownership and management responsibilities, ensure data quality, and provide the systems and supporting resources required for data management. The Data Security Governance Center (DSGC) helps customers automatically identify and classify cloud-based data assets and assess associated security risks. DSGC is an integrated data security operations platform that supports sensitive data discovery, classification and grading, data mapping, and abnormal access analysis. It works in coordination with Tencent Cloud's security capabilities to

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				form a closed-loop data protection framework, maximizing security effectiveness for enterprises. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive internal data classification and grading standard, in accordance with which all data is uniformly classified and graded upon creation. Customer data is classified as high-security-level data within Tencent Cloud. For internal Tencent Cloud employees, unless the service selected by the customer requires processing of the customer's data, no employee will attempt to access any customer data. For data storage protection, Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				keys are managed through the integrated Key Management Service (KMS), which provides full lifecycle management. Key Management Service (KMS) uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect keys and supports key rotation to reduce the risk of compromise or misuse. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission.

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
30	44	Personal Data Protection	(1) Banks shall implement the principle of personal data protection when processing personal data. (2) In the event of specific circumstances that may increase risks to personal data owners, Banks shall conduct an impact assessment on the implementation of the personal data protection principle referred to in paragraph (1). When conducting information technology operations, non-bank financial institutions must ensure that: a. The collection, processing, use, storage, updating and/or disclosure of consumers' personal data are based on the consent of the relevant consumers, except as otherwise provided by applicable laws and regulations; b. The use or disclosure of consumers' personal data is consistent with the purposes explained to the consumers at the time of data collection.	When processing personal data, customers shall comply with the principles of personal data protection. Under specific circumstances, customers shall conduct personal data privacy impact assessments. In addition, customers shall implement personal data protection requirements in data exchange activities, classify personal data, clarify the rights and obligations of relevant parties involved in personal data exchange, formulate personal data exchange agreements to confirm the methods of personal data exchange, and ensure the security of personal data. Customers shall ensure that they have obtained the consent of customers and potential customers when conducting personal data exchange. To assist customers in complying with regulatory requirements, Tencent Cloud provides an online Privacy Policy, which clearly states that Tencent Cloud will process data in accordance with applicable laws and regulations both in the course of providing Tencent Cloud services and under any other circumstances. On this basis, Tencent Cloud regards personal data compliance as a top priority in the service provision process, and adopts universally recognized personal data compliance principles (such as legality, fairness, transparency, purpose limitation, data minimization, integrity, accuracy, confidentiality, and accountability) as
N/A	45	Personal Data Exchange	(1) When implementing personal data protection in data exchange activities,	

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
			Banks shall establish at least: a. classification of data that constitutes personal data; b. rights and obligations of parties involved in personal data exchange; c. personal data exchange agreements; d. personal data exchange means; and e. personal data security. (2) The personal data exchange referred to in paragraph (1) shall be conducted with consideration of the consent of customers and/or prospective customers, implemented in accordance with the provisions of laws and regulations.	the guiding philosophy for privacy compliance. These principles are integrated into all stages of product design and development as well as the entire lifecycle of personal data, making privacy compliance an inherent attribute of the products. In addition, Tencent Cloud strictly complies with applicable privacy protection laws and regulations in countries and regions around the world, with a primary focus on the full lifecycle management of personal data, and has incorporated key compliance requirements such as Privacy by Design (PbD), data subject right response, and personal data disclosure. Tencent Cloud's years of security experience and accumulation have ensured the security of the cloud platform infrastructure and laid a solid foundation for the privacy compliance of customers' businesses. Tencent Cloud has established a comprehensive internal data classification and grading standard, in accordance with which all data is uniformly classified and graded upon creation. Customer data is classified as high-security-level data within Tencent Cloud. For internal Tencent Cloud employees, unless the service selected by the customer requires processing of the customer's data, no employee will attempt to access any customer data. Tencent Cloud has ensured the accuracy of data transmitted through its platform by means of access control, integrity

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
				verification and other measures. In addition, Tencent Cloud provides customers with communication channels that enable them to independently correct or delete any relevant inaccurate data. When obtaining customer consent for data processing, where Tencent Cloud acts as a data controller, it collects information provided by customers when registering for Tencent Cloud services, as well as data generated during interactions with Tencent Cloud in this process. In such cases, Tencent Cloud will fulfill its obligations as a data controller in accordance with its Privacy Policy. Where Tencent Cloud acts as a data processor, customers use Tencent Cloud's products or services to process data collected for their own business purposes. In such cases, Tencent Cloud is not only responsible for the functionality and security of its products or services, but also fulfills the relevant obligations of a data processor in accordance with the Data Processing and Security Agreement. In addition, all communications of customers on the Tencent Cloud console are protected by HTTPS secure protocol encryption. The cloud API interfaces provided by Tencent Cloud's cloud products also have security capabilities such as HTTPS encryption, signature verification, and status monitoring, providing port-level communication security assurance for

No.				
Nonbank				
Financial Service Institutions (NBFIs)	Commercial Banks	Domain	Summary of Controls	Tencent Cloud's Response
31	60	Interim Reports	(1) In the event of an IT incident that potentially causes and/or has caused significant losses and/or disrupts the smooth operation of the Bank, the Banks and Financial Institutions shall submit: a. an initial notification no later than 24 hours after becoming aware of the IT incident; and b. an IT incident report no later than 5 working days after becoming aware of the IT incident. (2) The initial notification specified in paragraph (1) letter a shall be submitted in writing via electronic means to the Financial Services Authority, based on available initial information.	customers' businesses. Customers should be aware that for information technology incidents that may cause significant losses or disrupt the operations, they must report to the financial regulatory authority through electronic channels within 24 hours, and submit a written report within the latest 5 working days. To support customers in meeting regulatory requirements, Regarding incident communication and notification, Tencent Cloud has developed an information security incident management standard, which includes procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. Tencent Cloud offers online chat and telephone support via the cloud console and official website, allowing

No.		Domain	Summary of Controls	Tencent Cloud's Response
Nonbank Financial Service Institutions (NBFIs)	Commercial Banks			
				customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates geographically redundant customer service centers, providing 24/7 support to handle customer requests, deliver round-the-clock technical assistance for cloud products, and ensure timely, high-quality service responses. Customers may also select an appropriate support plan, which can include access to dedicated support groups, a designated technical account manager, and value-added services for enhanced assistance.

07

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of the Regulation of the Cyber Resilience and Security for Commercial Banks

With the large-scale application of information technology, one of the potential risks is that arising from cyber threats and cyber incidents. Banks are not only required to ensure that their electronic systems are protected against cyberattacks, but also to be equipped with the capabilities of detection and recovery following the occurrence of cyber incidents. In response to this, the Indonesian Financial Services Authority (OJK) formulated and issued Circular No. 29/SEOJK.03/2022 on [Cyber Resilience and Security for Commercial Banks](#), to guide banks in establishing a sound and secure operational system. Among its appendices, Appendix Ib: Quality Assessment for Cybersecurity Risk Implementation and Appendix Ic: Quality Assessment for Cybersecurity Resilience Implementation specify that banks shall implement sound governance and risk management, ensure operational continuity through the appropriate application of information technology, and safeguard cybersecurity and resilience. The provisions primarily focus on the cybersecurity risk management framework, cybersecurity risk management processes, adequacy of human resources, assets, threat and vulnerability identification processes, asset protection processes, cyber incident detection processes, and cyber incident response and recovery processes.

In this chapter, Tencent Cloud will extract and summarize the control requirements relevant to cloud service providers as set forth in Appendix Ib and Appendix Ic of Circular No. 29/SEOJK.03/2022 on Cyber Resilience and Security for Commercial Banks, and elaborate on how Tencent Cloud, as a cloud service provider, can assist commercial banks in complying with these requirements.

7.1 Quality Assessment for Cybersecurity Risk Implementation

No.	Domain	Summary of Controls	Tencent Cloud's Response
1.3	Cybersecurity Risk Management Policy	c. The Bank shall ensure that all employees and stakeholders fully understand and effectively implement cybersecurity policies.	Customers shall ensure that all employees and stakeholders fully understand and effectively implement cybersecurity policies. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. Tencent Cloud conducts information security and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			personal data protection training for all business units at least once a year and requires personnel to confirm annually that they have read and understood security policies and procedures.
2.1	Cybersecurity Risk Management Policy	a. The Bank shall formulate a cybersecurity-related risk management strategy that aligns with the Bank's vulnerabilities, exposure to cyber threats, cybersecurity-related risk appetite and risk tolerance, and overall business strategy. b. The Bank shall clarify all roles and responsibilities related to cybersecurity in the cybersecurity-related risk management strategy.	Customers shall formulate cybersecurity risk management strategies, clarify cybersecurity roles and responsibilities, align such strategies with the company's risk appetite and risk tolerance, and keep them consistent with the company's overall strategy. o support customers in meeting regulatory requirements, Tencent Cloud has defined an Information Security Risk Management Procedure, which provides clear defines for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessments at least annually, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. Furthermore, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices.
2.3	Cybersecurity Policies and Procedures	c. The Bank shall integrate cybersecurity-related risk management policies—including cybersecurity-related risk management strategies and objectives—into business processes across all business lines and support activities.	Customers shall establish cybersecurity policies and procedures tailored to the characteristics and complexity of business activities, and integrate them into the business processes of all business lines and support functions. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.3	Asset Protection	This includes developing specific policies to meet the needs of individual business lines and support activities. d. The Bank shall formulate adequate cybersecurity-related risk management policies. e. The Bank shall have procedures derived from cybersecurity-related risk management policies. These procedures may include general controls applicable to all business lines and support activities, as well as specific controls tailored to individual business lines and support activities.	comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy.
		f. The Bank shall have cybersecurity policies and procedures for governing the protection of IT assets.	Customers shall develop cybersecurity policies and procedures related to IT asset protection. To assist customers in comprehensive information asset management, Tencent Cloud provides <u>Cloud Workload Protection Platform (CWPP)</u>, which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, <u>Cloud Security Center (CSC)</u>, for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such as cloud configuration risks,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. To support customers in meeting regulatory requirements, Tencent Cloud has formulated information asset management specifications and full-lifecycle management processes, which conduct classified and hierarchical management and protection of assets such as electronic data, hardware and their virtual devices, infrastructure, application systems, and software. Tencent Cloud manages hardware devices and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, etc. This ensures the stable operation of the underlying system of the cloud platform and provides reliable support for business systems.
2.3	Third-Party Management	g. The Bank shall have cybersecurity-related risk management policies and procedures for third parties and third-party subcontractors. These policies and procedures shall govern the management of the Bank's digital data/information (including customer data held by the Bank) by third parties and third-party subcontractors. h. The Bank shall implement cybersecurity-related risk management for third parties and third-party subcontractors. i. The Bank shall establish minimum cybersecurity control standards for third parties and third-party subcontractors, which include: 1. Confidentiality provisions in	Customers shall formulate cybersecurity management policies and procedures for third parties and their subcontractors, including specifying confidentiality clauses in cooperation agreements, requiring third parties and their subcontractors to establish cybersecurity governance mechanisms, and mandating the implementation of cybersecurity risk management practices. Tencent Cloud makes available a suite of legal documents on its official international website, including the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings provided by Tencent Cloud, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, as well as service terms and scenarios for agreement termination. Customers may also opt to sign offline agreements with Tencent Cloud to negotiate and finalize the specific terms and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		cooperation agreements;	detailed provisions thereof.
		2.The availability of cybersecurity governance (policies, procedures, regulations, etc.) at third parties and third-party subcontractors; and	Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system.
		3.Cybersecurity-related risk management (including cyber incident management) at third parties and third-party subcontractors.	The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. In addition, Tencent Cloud undergoes annual professional audits conducted by independent third parties both at home and abroad. By providing attestation-based System and Organization Controls (SOC) reports, we disclose the latest internal control status of our service organization to cloud user institutions, independent auditors, regulatory authorities, corporate shareholders and other relevant stakeholders. Furthermore, for subcontracting scenarios, the agreements also include clauses governing prior consent for subcontracting, notification requirements prior to adding or replacing subcontractors, and data protection obligations. Without the customer's prior written consent, Tencent Cloud shall not subcontract any

No.	Domain	Summary of Controls	Tencent Cloud's Response
			processing operations performed on behalf of the customer pursuant to the contract or agreement. In the event of any intended changes involving the addition or replacement of subcontractors, Tencent Cloud will notify the customer via email or other designated channels. In terms of subcontractor management, Tencent Cloud has established a robust supply chain security management system. Through rigorous supplier security assessment and onboarding, regular supervision and evaluation, and clearly defined outsourcing service agreements, Tencent Cloud implements effective control over suppliers. This ensures that subcontracting activities will not compromise Tencent Cloud's ability to provide relevant services to customers, the confidentiality and integrity of customer information processing, as well as the supervision and audit rights of Indonesia's financial regulators and financial institutions. In addition, Tencent Cloud will actively comply with customers' outsourcing management requirements and fully respond to and cooperate with audit or assessment activities initiated by customers.
3.1	Cybersecurity Risk Management Processes (Identification, Measurement, Monitoring and Control)	a. The Bank shall conduct periodic identification of all cybersecurity-related risks. b. The Bank shall ensure the availability of methods or systems for identifying risks in all Bank activities related to cybersecurity. c. The Bank shall conduct periodic risk measurement for all Bank activities related to cybersecurity. f. The Bank shall have systems and procedures for monitoring cybersecurity-related risks.	Customers shall conduct periodic cybersecurity risk assessments, establish systems to identify cybersecurity risks, carry out risk measurement for cybersecurity-related business activities, and set up risk monitoring systems and procedures for cybersecurity. To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. • Risk Identification: Tencent Cloud conducts risk assessments regularly,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			identifying applicable risk scenarios from sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. • Risk Assessment: Tencent Cloud evaluates asset value, the likelihood of risk scenarios, and the potential impact, then calculates the risk level. • Risk Treatment: Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items, the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored. • Risk Monitoring, Review, and Reporting: Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.2	Cybersecurity Human Resources	b. The Board of Directors shall develop systems for employee recruitment, development, and training. This includes managerial succession planning and adequate remuneration to ensure the availability of competent employees in cybersecurity-related risk management. c. The Board of Directors shall ensure that all HR personnel have adequate understanding of cybersecurity-related risks. They shall also be able to communicate the implications of cybersecurity-related risks to the Board of Directors, Board of Commissioners, management, and customers. d. The Board of Directors shall ensure that all HR personnel understand the cybersecurity strategy, cybersecurity-related risk appetite and risk tolerance, and the cybersecurity-related risk management framework established by the Board of Directors and approved by the Board of Commissioners. It shall also ensure that all HR personnel consistently implement these in their respective activities. f. The Bank shall develop and implement a continuous program to enhance cybersecurity-related capabilities for all relevant employees. This includes personnel at the Board of Directors, Board of	Customers shall establish a system for personnel recruitment, development and training to conduct appropriate management of their staff, including implementing staff selection processes, signing confidentiality agreements with employees, and establishing management mechanisms for promoting awareness of information technology risks. To support customers in meeting regulatory requirements, Tencent has established comprehensive HR management standards and procedures to ensure personnel are selected, recruited, and assigned according to job requirements. Tencent Cloud has implemented a clear employee lifecycle management process, including onboarding, employment, and offboarding procedures. Before employment, applicants undergo interviews to assess their suitability for the role. Based on applicable laws and job level, the HR department conducts background checks prior to hiring. These checks include verification of past employment history, criminal background, and academic qualifications. The results are recorded in Tencent Cloud's HR management system. Upon employment, internal staff must sign an employment agreement and a confidentiality agreement. The employment agreement specifies Tencent Cloud's security policies and the responsibilities of employees or third-party personnel regarding information security and personal data protection. The confidentiality agreement outlines confidentiality obligations and penalties for violations. Outsourced staff are also subject to background checks and bound by employment and confidentiality requirements stipulated in agreements between Tencent Cloud and the outsourcing vendor. Legal teams review and update confidentiality requirements as needed. In terms of information security training and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Commissioners, and management levels—to ensure each employee has the competence and expertise to effectively perform their roles and responsibilities. g. The Bank shall conduct a gap analysis to understand employees' level of knowledge and capabilities related to cybersecurity. It shall use this information to develop an action plan for enhancing employee capabilities.	awareness promotion , Tencent Cloud has established a comprehensive internal information security training mechanism, which mandates that regular employees, consultants, interns and contracted staff complete information security training courses. Relevant training programs include mandatory training for all staff, specialized training for key positions, and optional professional courses, covering areas such as basic security awareness, office security, vulnerability identification and defense, privacy protection, emergency response, R&D security standards, and data security requirements. Tencent Cloud conducts information security and personal data protection training for all business units at least once a year and requires personnel to confirm annually that they have read and understood security policies and procedures.
4.2	Reviews and Assessment	a. The Bank shall conduct periodic reviews and evaluations of the implementation of cybersecurity-related risk management, in accordance with the Bank's characteristics and complexity b. The Bank shall ensure that the department responsible for cybersecurity-related risk management functions conducts adequate reviews and evaluations. c. The Bank shall ensure that the internal audit department conducts adequate reviews and evaluations. d. The Bank shall ensure that the parties conducting reviews and evaluations of cybersecurity-related risk management implementation	Customers shall establish an information technology audit mechanism, conduct regular reviews and evaluations of the implementation of cybersecurity risk management, ensure that auditors possess professional competence and skills, and report the results of such reviews and evaluations to the management. To support customers in meeting regulatory requirements, Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. In addition, Tencent Cloud undergoes annual professional audits conducted by independent third parties both at home and abroad. By providing attestation-based System and Organization Controls (SOC) reports, we disclose the latest internal control status of our

No.	Domain	Summary of Controls	Tencent Cloud's Response
		have strong independence, competence, and reliable review methods.	service organization to cloud user institutions, independent auditors, regulatory authorities, corporate shareholders and other relevant stakeholders.
		e. The Bank shall ensure that the results of reviews and evaluations of cybersecurity-related risk management implementation are reported to the Board of Directors and the Board of Commissioners. This is to facilitate the development of corrective actions and/or improvements to cybersecurity-related risk management.	To ensure that Tencent Cloud's information technology policies, procedures, processes, and control measures meet the requirements of Indonesian financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Indonesian financial industry conducted by an independent third party. Customers can independently download the latest report from the Tencent Cloud Compliance Document Center .

7.2 Quality Assessment for Cybersecurity Resilience Implementation

No.	Domain	Summary of Controls	Tencent Cloud's Response
1.a	Asset Management	a. The Bank shall implement asset management through effective inventory and assessment of IT assets (including hardware, software, networks, and infrastructure) as well as configuration documentation.	Customers shall conduct effective inventory-taking and assessment of IT assets, and document their configuration information. To assist customers in comprehensive information asset management, Tencent Cloud provides Cloud Workload Protection Platform (CWPP), which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, Cloud Security Center (CSC), for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			risks through multiple security dimensions such as cloud configuration risks, vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. To support customers in meeting regulatory requirements, Tencent Cloud has formulated information asset management specifications and full-lifecycle management processes, which conduct classified and hierarchical management and protection of assets such as electronic data, hardware and their virtual devices, infrastructure, application systems, and software. Tencent Cloud manages hardware devices and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, etc. This ensures the stable operation of the underlying system of the cloud platform and provides reliable support for business systems.
1.b	Vulnerability Management	b. The Bank shall identify vulnerabilities and monitor the latest cyber developments to detect cyber threats.	Customers shall identify vulnerabilities, monitor the latest cyber developments, and detect cyber threats. For vulnerability scanning, customers can use the Vulnerability Scanning Service (VSS) to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation advice to reduce security risks. VSS can integrate with other Tencent Cloud products such as Host Security and Web Application Firewall to achieve a closed-loop process from risk monitoring to risk mitigation. To support customers in threat detection and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			analysis, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. In addition, TIX is SaaS-based and supports multiple delivery methods, including web portals, APIs, SDKs, TIP integration, and mini-programs, meeting varied customer needs. It can also integrate with customers' existing security products to enhance overall security operations and threat response efficiency.
1.c	Cybersecurity Testing	c. The Bank shall conduct periodic cybersecurity testing.	Customers shall conduct periodic cybersecurity tests. In terms of penetration testing, Tencent Cloud provides customers with Penetration Testing Service (PTS). By fully simulating attack techniques and vulnerability discovery methods that may be employed by hackers, PTS adopts controlled and non-destructive approaches to conduct in-depth security detection on target systems, identify vulnerabilities existing in targets and network devices, and provide security hardening recommendations to help customers enhance system security and support verification after vulnerability remediation. For vulnerability scanning, customers can opt for Vulnerability Scanning Service (VSS) to detect enterprise network assets and identify their risks. Leveraging Tencent's years of accumulated

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security experience and threat intelligence, VSS has established a comprehensive and robust vulnerability rule database, and is equipped with professional and efficient 0Day/1Day/NDay vulnerability detection capabilities. It can perform regular security scans, continuous risk alerts, and vulnerability detection on the availability, security, and compliance of customer assets, provide customers with professional remediation recommendations, and mitigate security risks. VSS also supports integration with cloud products such as host security and web application firewalls, forming a closed loop from risk monitoring to risk disposal. To assist customers in complying with regulatory requirements, Tencent Cloud regularly generates scanning tasks through its vulnerability scanning system to conduct vulnerability scans on assets in the cloud environment, and performs analysis, classification, and remediation of detected vulnerabilities. In addition, Tencent Cloud conducts periodic full-link large-scale penetration tests to proactively identify and remediate potential system security risks at an early stage, and flexibly carries out targeted penetration tests prior to the launch of new products or in the event of material changes. Penetration test results are notified to the relevant responsible departments via security tickets, and the responsible departments shall promptly carry out vulnerability remediation or implement other compensating control measures to ensure that exploitable vulnerabilities identified in penetration tests are properly addressed. Furthermore, Tencent Cloud conducts regular red team-blue team exercises to simulate real-world cyberattack defense drills. Tencent Cloud has also established an external vulnerability feedback platform and launched a bug bounty program, inviting industry security experts to help identify system security vulnerabilities and risks from a hacker's perspective, so as to remediate security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			issues in a timely manner and maintain the security of the Tencent Cloud ecosystem.
			Customers shall formulate cybersecurity control measures based on the results of risk assessments, implement standardized and well-managed security systems, conduct regular reviews and updates of cybersecurity control measures, and ensure the adequacy of the security control measures in use in accordance with applicable policies and procedures.
			To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy.
2.a	Security	a. The Bank shall implement comprehensive security controls based on the results of asset, threat, and vulnerability identification.	
2.b	Control	b. The Bank shall maintain and remediate security controls for IT assets in accordance with applicable policies and procedures.	
2.c、2.d	Measures	c. The Bank shall implement well-managed security systems in line with applicable policies and procedures.	
		d. The Bank shall update its security controls periodically to ensure the adequacy of the security controls used, based on the latest identification results.	The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. In addition, Tencent Cloud undergoes professional audits conducted by independent third parties. By providing attestation-based System and Organization Controls (SOC) reports, we disclose the latest internal control status of our service organization to cloud user institutions,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			independent auditors, regulatory authorities, corporate shareholders and other relevant stakeholders. To ensure that Tencent Cloud's information technology policies, procedures, processes, and control measures meet the requirements of Indonesian financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Indonesian financial industry conducted by an independent third party. Customers can independently download the latest report from the Tencent Cloud Compliance Document Center.
2.e	Data and Information Security	e. The Bank shall implement data and information security management. It shall also ensure that data and/or information are managed in accordance with the organization's cybersecurity-related risk management strategy to protect the confidentiality, integrity, and availability of data and information.	Customers shall establish data security protection mechanisms, classify data according to its sensitivity and importance levels, implement data protection measures based on different data levels, and adopt trusted internationally recognized encryption standards to protect the confidentiality and integrity of data. To support customers in meeting regulatory requirements, in terms of data classification and grading, The Data Security Governance Center (DSGC) helps customers automatically identify and classify cloud-based data assets and assess associated security risks. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive internal data classification and grading standard, in accordance with which all data is uniformly classified and graded upon creation. Customer data is classified as high-security-level data within Tencent Cloud. For internal Tencent Cloud employees, unless the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			service selected by the customer requires processing of the customer's data, no employee will attempt to access any customer data. In terms of data storage protection, a variety of Tencent Cloud's storage and database products support data encryption functionality, adopting secure and high-strength encryption algorithms. They also implement full lifecycle management of keys through integration with the Key Management Service (KMS), ensuring data confidentiality. The Key Management Service (KMS) uses FIPS-140-2 certified Hardware Security Modules (HSM) to generate and protect keys, and supports the full lifecycle management of customer-encrypted keys. To reduce the risk of key compromise or misuse, KMS supports key rotation, and adopts secure and reliable methods to delete invalid, obsolete, or leaked keys. Deleted keys cannot be recovered, and encrypted data under such keys cannot be decrypted either. In addition, Tencent Cloud adopts multi-copy redundant storage and erasure coding technology when storing data, and immediately takes necessary recovery measures upon detection of integrity errors, which greatly improves the fault tolerance capability of data. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. For data deletion and destruction, Tencent Cloud provides a secure and reliable data destruction mechanism. Upon termination of the customer's services, Tencent Cloud will adhere to strict data erasure methods completely delete all customer data—including copies and backups—upon the expiration of the retention period, with no possibility of recovery of the deleted data. When the media used to provide Tencent Cloud services malfunctions and requires replacement or reaches the end of its service life and needs to be decommissioned, Tencent Cloud will also promptly erase residual information and carry out complete physical destruction in accordance with rigorous procedures.
2.f	Network, Hardware and Software Protection	f. The Bank shall implement protection management for networks, hardware, and software.	Customers shall implement network segmentation management based on the criticality of systems or the sensitivity of data, and deploy and install cybersecurity devices such as firewalls, intrusion prevention systems, and DDoS protection solutions. In addition, customers shall implement necessary protection measures for the hardware and software used in information systems. For network segmentation or partitioning, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access

No.	Domain	Summary of Controls	Tencent Cloud's Response
			control. To implement network boundary protection, Tencent Cloud provides the EdgeOne (EO) platform, which leverages Tencent's global edge nodes to deliver security and acceleration services, including DDoS protection, intelligent web defense, bot/crawler attack mitigation, and DNS resolution. EO also supports custom access control rules based on business needs. Customers can further enhance perimeter security using Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services. Cloud Firewall (CFW) offers ACL-based firewall control, IPS real-time interception, virtual patching, and malicious code detection, enabling granular isolation between VPCs and protecting core assets. Web Application Firewall (WAF) defends against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and malicious crawlers. Anti-DDoS combines abundant mitigation resources with AI-driven traffic cleansing algorithms to counter evolving DDoS threats. For secure network communication, customer interactions on the Tencent Cloud console are encrypted using HTTPS. VPN Connection enables secure transmission between on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet Key Exchange) and IPsec protocols to encrypt data, creating a secure and trusted channel over the Internet. Tencent Cloud has established network security management standards and a defense-in-depth architecture. Security domains are defined based on business functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time. In terms of hardware and software

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management, Tencent Cloud has established information asset management standards and lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems. Tencent Cloud regularly retires and replaces servers, and upgrades software components (such as operating systems and database systems) to appropriate versions before the end of their support lifecycle. For decommissioned hard drives, Tencent Cloud adopts secure physical destruction methods to ensure complete erasure, with all destruction activities recorded in official documentation.
2.g	Access Control	g. The Bank shall implement access and user protection management to prevent unauthorized actions on devices, network infrastructure, and system components managed by the Bank.	Customers shall establish identity authentication and access control mechanisms for data and information technology systems to regulate access to information assets, conduct periodic reviews and updates of permissions, and strengthen the security management of privileged user accounts. In terms of user account and authorization management, Cloud Access Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources. Through the CAM console, customers can configure password policies for sub-users, including complexity, length, and validity period. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to customer passwords, ensuring that plaintext passwords are never stored. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive

No.	Domain	Summary of Controls	Tencent Cloud's Response
			operations. Tencent Cloud has also implemented an access control authorization policy and a role-separation matrix mechanism. It requires user accounts to use unique identifiers and sets password policies for employee accounts based on security baselines, including password length, complexity, locking, and resetting. For internal terminals, operating systems, applications, and network devices, Tencent Cloud has configured policies for limiting the number of failed login attempts and session timeouts. Tencent Cloud uses a zero-trust security management system to authenticate employee access, requiring users to complete two-factor authentication through the system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions to employees only based on job responsibilities and business necessities. Regular permission reviews are conducted to prevent permission misuse and abuse. For high-privilege users, Customers can use Cloud Access Management (CAM) to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Tencent Cloud has also clearly defined the management requirements for special access permissions and established relevant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			authorization mechanisms. Tencent Cloud's production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before accessing bastion hosts, and only authorized personnel can log in after completing secondary identity verification.
2.h	Engagement of IT Service Providers	h. The Bank shall implement adequate protection in its cooperation with IT service providers, including in cloud usage.	When collaborating with IT service providers, including cloud service providers, customers shall implement adequate protection measures. Upholding the open and shared nature of cloud computing services, Tencent Cloud continuously enhances the security capabilities of its cloud platform and services, and works together with customers to build a more robust and comprehensive security system for cloud-based businesses and data. As a cloud service provider, Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Considering that customers have varying levels of control over different components depending on the cloud service models they choose (e.g., IaaS, PaaS, and SaaS), Tencent Cloud has established a Cloud Security Shared Responsibility Model based on different cloud service categories. For details, please refer to Chapter 3 of this guideline: Tencent Cloud Security Responsibility Sharing Model. Tencent Cloud designs and builds its cloud services in accordance with internationally recognized information security and IT governance standards, and strictly complies with the data security and privacy protection laws and regulations of the jurisdictions where it operates. Tencent Cloud has obtained multiple international security compliance certifications, providing customers with cloud products and services verified by authoritative third-party certification bodies.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud makes available a suite of legal documents on its official international website, including the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings provided by Tencent Cloud, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also opt to sign offline agreements with Tencent Cloud to negotiate and finalize the specific terms and detailed provisions thereof. Tencent Cloud actively complies with customers' outsourcing management requirements, assigns dedicated personnel to assist with audits or assessments initiated by customers, and provides a variety of security protection measures and related cloud products/services to ensure the confidentiality and integrity of customers' cloud-based data.
2.i	Secure Coding	i. The Bank shall ensure the implementation of secure coding in system and application development to minimize vulnerabilities in systems and applications.	Customers shall adopt security measures such as secure coding standards and source code reviews to prevent software vulnerabilities or defects. Cloud-Native Build (CNB) provides a complete developer toolchain with capabilities including code hosting, high-performance R&D pipelines, AI code assistants, and artifact management. Its AI code assistant is an AI-powered programming tool designed specifically for developers by Tencent Cloud. Supporting multiple mainstream programming languages, it offers features such as code completion, unit testing, code diagnosis, intelligent code reviews, and AI-powered Q&A for coding issues, aiming to help developers improve coding quality and efficiency. For secure coding and code reviews, Tencent Cloud has formulated detailed secure coding standards that all internal developers must strictly follow. It also conducts secure programming

No.	Domain	Summary of Controls	Tencent Cloud's Response
			training to enhance developers' awareness of risks such as injection attacks and sensitive data leakage. Developers are required to incorporate security features into application systems during the development phase to minimize vulnerabilities. Tencent Cloud's internal code security inspection and analysis solution integrates multiple capabilities including Static Application Security Testing (SAST), open-source component vulnerability detection, and sensitive information scanning. Business teams can seamlessly integrate these scanning capabilities into their R&D pipelines to conduct security assessments of code submissions at the code admission stage. Typical issues identified during code reviews are documented and compiled into the business teams' knowledge bases. Code review standards mainly cover detection of multi-language vulnerabilities (such as XSS, SQL injection, code execution, and command injection), historical vulnerabilities in third-party open-source components, and sensitive information protection.
2.j	Patch Management	j. The Bank shall ensure the proper execution of patching. It shall also ensure the reliability and updating of all software components, communication networks, databases, and the Bank's operating systems.	Customers shall establish a patch management process, and deploy patches based on the severity of vulnerabilities and the importance of IT systems, to ensure the reliability and timely updating of all software components, communication networks, databases, and banking operating systems. Customers can use Cloud Workload Protection Platform (CWPP) to detect vulnerabilities in Linux software, Windows systems, Web-CMS platforms, and applications, issue real-time alerts, and provide vulnerability remediation solutions, helping customers respond quickly to vulnerability risks. Tencent Container Security Service (TCSS) integrates a virtual patching system developed by Tencent Cloud Security to defend against emerging zero-day vulnerabilities. It can capture and analyze vulnerabilities, generate virtual patches based on Tencent's

No.	Domain	Summary of Controls	Tencent Cloud's Response
			expertise, and automatically deploy these virtual patches on cloud servers, effectively blocking hacker attacks. In addition, customers can use Vulnerability Scanning Service (VSS) to conduct regular security scans, continuous risk alerts, and vulnerability detection on the availability, security, and compliance of enterprise network devices and application services, and leverage VSS's professional remediation recommendations to mitigate enterprise security risks. To support customers in meeting regulatory requirements, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Tencent Cloud also operates internal vulnerability scanning and external vulnerability reporting platforms to track and remediate issues. Security tickets are logged in the operations system and assigned to responsible teams for timely resolution. In addition, Tencent Cloud's security research team integrates virtual patching capabilities into its Web Application Firewall to enhance overall platform security.
3.a	Security Baselines	a. The Bank shall ensure the availability of baseline performance documentation for the Bank's critical functions and supporting systems. This enables the timely detection of any deviations and the flagging of anomalous activities or events for follow-up.	Customers shall formulate security standards for the hardware and software supporting critical systems, implement secure configurations, and establish relevant processes to verify deviations between system configurations and security standards. Tencent Cloud's Cloud Security Center (CSC) provides automated configuration risk assessment capabilities to help customers reduce security risks caused by misconfigurations and improve overall cloud security posture. Customers can also use Config Audit to perform centralized auditing and governance of cloud resources, continuously recording configuration details and changes across different regions under their account. Based on Tencent Cloud best practices and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. To support customers in meeting regulatory requirements, Tencent Cloud has established a Configuration Management Policy and uses a Configuration Management Database (CMDB) to centrally manage IT service components and configuration items (CIs), including their relationships. When configuration updates occur during change processes, operations personnel update the version and related information of configuration items in the CMDB according to the change plan. Tencent Cloud conducts regular asset inventories and audits the CMDB to ensure the validity, accuracy, and completeness of configuration information. In addition, Tencent Cloud has established configuration and baseline standards to standardize security settings for network devices, firewalls, servers, operating systems, databases, and applications. Continuous scanning tools detect deviations from standards in operating systems, database management systems, and virtual images. Identified deviations automatically generate security tickets for timely remediation. Security teams also review network device policies and parameters regularly to ensure effectiveness.
3.b	Security Monitoring	b. The Bank shall monitor suspicious activities and manage and test detection processes and procedures to ensure the timely detection of anomalous activities.	Customers shall establish cybersecurity situational awareness capabilities to monitor emerging threats, and detect abnormal events and threats affecting critical systems, ensuring timely detection, prevention, and response. To support customers in threat detection and analysis, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface

No.	Domain	Summary of Controls	Tencent Cloud's Response
			intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. In addition, TIX is SaaS-based and supports multiple delivery methods, including web portals, APIs, SDKs, TIP integration, and mini-programs, meeting varied customer needs. It can also integrate with customers' existing security products to enhance overall security operations and threat response efficiency. Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable.
3.c、3.e	Vulnerability Detection	c. The Bank shall continuously monitor or detect vulnerabilities to ensure the effectiveness of the implemented protection measures. e. The Bank shall analyze the threats and vulnerabilities associated with a cyber incident to ensure effective incident	Customers shall conduct continuous vulnerability monitoring or detection to ensure the effectiveness of implemented protection measures. In terms of penetration testing, Tencent Cloud provides customers with Penetration Testing Service (PTS). By fully simulating attack techniques and vulnerability discovery methods that may be employed by hackers, PTS adopts controlled and non-destructive approaches to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		handling, thereby preventing disruptions to the Bank's services and/or operations.	conduct in-depth security detection on target systems, identify vulnerabilities existing in targets and network devices, and provide security hardening recommendations to help customers enhance system security and support verification after vulnerability remediation. For vulnerability scanning, customers can opt for Vulnerability Scanning Service (VSS) to detect enterprise network assets and identify their risks. Leveraging Tencent's years of accumulated security experience and threat intelligence, VSS has established a comprehensive and robust vulnerability rule database, and is equipped with professional and efficient 0Day/1Day/NDay vulnerability detection capabilities. It can perform regular security scans, continuous risk alerts, and vulnerability detection on the availability, security, and compliance of customer assets, provide customers with professional remediation recommendations, and mitigate security risks. VSS also supports integration with cloud products such as host security and web application firewalls, forming a closed loop from risk monitoring to risk disposal. To assist customers in complying with regulatory requirements, Tencent Cloud regularly generates scanning tasks through its vulnerability scanning system to conduct vulnerability scans on assets in the cloud environment, and performs analysis, classification, and remediation of detected vulnerabilities. In addition, Tencent Cloud conducts periodic full-link large-scale penetration tests to proactively identify and remediate potential system security risks at an early stage, and flexibly carries out targeted penetration tests prior to the launch of new products or in the event of material changes. Penetration test results are notified to the relevant responsible departments via security tickets, and the responsible departments shall promptly carry out vulnerability remediation or implement other compensating control measures to ensure that

No.	Domain	Summary of Controls	Tencent Cloud's Response
			exploitable vulnerabilities identified in penetration tests are properly addressed. Furthermore, Tencent Cloud conducts regular red team-blue team exercises to simulate real-world cyberattack defense drills. Tencent Cloud has also established an external vulnerability feedback platform and launched a bug bounty program, inviting industry security experts to help identify system security vulnerabilities and risks from a hacker's perspective, so as to remediate security issues in a timely manner and maintain the security of the Tencent Cloud ecosystem.
3.d	Incident Detection	d. The Bank shall ensure the availability of adequate processes for detecting cyber incidents.	Customers shall implement centralized monitoring of security incidents and accidents in cloud environments to ensure timely detection and response to security events in the cloud. Customers can leverage Cloud Log Service (CLS), a one-stop log management platform that offers a full suite of capabilities including log collection, storage, search and analysis, real-time consumption, and log delivery. It helps customers address challenges in business operations, security monitoring, log auditing, and log analysis. Cloud Security Center (CSC) centrally aggregates various cloud-native security-related data, such as alerts from cloud security products, cloud asset configuration changes, user operation behaviors on the cloud, and logs from select cloud products. It also provides a unified search and investigation platform, enabling customers to achieve comprehensive log auditing and search capabilities for their cloud environments. In addition, customers can utilize Elasticsearch Service (ES) to ingest real-time logs from cloud servers, containers, and other cloud products, as well as historical and incremental business data, into Tencent Cloud ES clusters for distributed data storage, query, and analysis. To assist customers in meeting regulatory requirements, Tencent Cloud has established a Security Operations Center (SOC) built on cloud-

No.	Domain	Summary of Controls	Tencent Cloud's Response
			native technologies. Focusing on threat detection, investigation, and response, the center enhances security operation efficiency and ensures the overall network security posture is knowable, visible, and controllable. A dedicated team performs professional security operations on a 24/7 basis, enabling rapid response to and handling of security alerts, completion of preliminary analysis, and formulation of containment strategies to prevent attacks or security incidents from occurring.
4a-f	Cybersecurity Incident Response and Recovery	a. The Bank shall establish a cyber incident response and recovery plan. This plan shall ensure timely response and service restoration in line with the risks posed, with minimal impact. b. The Bank shall define the roles, tasks, and responsibilities of the cyber incident response team. This ensures that cyber incident response and recovery are implemented with minimal impact on the Bank's services and operations. c. The Bank shall implement recovery procedures and take measures to prevent the spread of the impact of a cyber incident by mitigating the impact and addressing the cyber incident. d. The Bank shall conduct analysis to ensure that cyber incident response and recovery steps are implemented correctly. e. The Bank shall escalate and report cyber incidents in accordance with established	Customers shall formulate a cybersecurity incident response and recovery plan, clarify the roles and responsibilities of the cybersecurity incident response team, implement recovery procedures when incidents occur to mitigate their impacts, establish communication channels for reporting cybersecurity incidents, and conduct post-incident analysis and evaluation to ensure the accuracy of response actions, summarize lessons learned, and drive continuous improvement. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—Cloud Security Center (CSC). Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the efficiency of security operations. For incident management, Tencent Cloud has established incident and service request management procedures and formulated an incident management policy. This ensures that all incidents related to IT service management activities are recorded and categorized, prioritized based on impact and urgency, and escalated as needed to ensure rapid resolution and closure. These measures minimize the impact of incidents,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		communication channels.	maintain normal business operations, and enhance customer satisfaction.
		f. The Bank shall conduct post-incident analysis to derive lessons learned from cyber incident response and recovery, for continuous improvement.	Regarding incident communication and notification, Tencent Cloud has developed an information security incident management standard, which includes procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. For incident summary and continuous improvement, Tencent Cloud has established a periodic incident analysis mechanism. It conducts multi-dimensional analysis of incidents (including incident type, frequency, impact scope, and severity) on a regular basis, and implements preventive measures based on incident reviews and root cause analysis to avoid recurrence of similar events. For major security incidents, Tencent Cloud will set up a dedicated task force to produce a special analysis report and submit it to the senior management. Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline

No.	Domain	Summary of Controls	Tencent Cloud's Response
			support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.

08

Conclusion

Tencent Cloud is a cloud computing brand developed by Tencent Group, leveraging years of technical expertise and security practices. Tencent Cloud is committed to providing customers with a secure, trusted, and intelligent cloud platform, helping enterprises efficiently embrace digital transformation and advance secure business development.

Based on the key regulatory requirements of the Indonesian Financial Services Authority (OJK), this guideline comprehensively and transparently demonstrates how Tencent Cloud assists customers in achieving compliance for their cloud-based systems and data, empowering enterprise customers to host their systems and data on the cloud with full confidence and peace of mind. Through this guideline, Tencent Cloud aims to support enterprise customers in effectively meeting the compliance standards of the Indonesian Financial Services Authority, while facilitating their efficient digital transformation and innovative business development.

This guide is for reference only. Customers should adapt the information herein to their specific circumstances to ensure regulatory compliance when using Tencent Cloud services.

09

Version History

Date	Version	Detail
April 2026	V1.0	Initial Release