



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

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	6
2.2	ISO/IEC Certification	6
2.3	Regional and Industry Compliance.....	8
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 FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition)	
5.1	Control Standards.....	19
5.1.1	Internal Control	19
5.1.2	External Control	33
5.2	Practice Standards	49
5.2.1	Information Security	49
5.2.2	General System Operation and Maintenance.....	78
5.2.3	Operational Control.....	90
5.2.4	Management of Various Types of Equipment.....	104
5.2.5	Emergency Response.....	118
5.2.6	System Development and Change.....	126
5.2.7	Measures for Enhancing System Reliability	131
5.2.8	Individual Businesses and Services, Etc.	150
5.3	Equipment Standards	156
5.3.1	Data Centers	156
5.4	Audit Standards	157
5.4.1	System Audit.....	157
06	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Cybersecurity for the Financial Sector	
6.1	Establishment of Cybersecurity Management System	161
6.2	Identification of Cybersecurity Risks	168
6.3	Defense Against Cyberattacks	181
6.4	Detection of Cyberattacks.....	206
6.5	Response and Recovery from Cyber Incidents.....	209
6.6	Third-Party Risk Management.....	216
07	How Tencent Cloud Complies with the Payment Services Act	
08	Conclusion	
09	Version History	

01

Overview

With the rapid development of new digital technologies and services, the information systems of Japanese financial institutions and related entities are becoming increasingly complex, and the number of cloud service providers and FinTech companies providing services to these institutions and entities is also increasing. These changes bring new risks: firstly, financial system disruptions caused by cybersecurity incidents may have broader and more severe impacts than before; Secondly, cyber-attacks targeting key data such as customer information held by financial institutions and related entities are also showing an increasingly complex and large-scale trend. In order to prevent cyber threats from harming the interests of financial service users and maintain financial system stability, the Financial Service Agency (FSA) and The Center for Financial Industry Information Systems (FISC) actively promote the strengthening of cybersecurity in the entire financial industry. They have issued multiple cybersecurity related standards and guidelines, requiring financial institutions to implement sufficient security measures to ensure their cybersecurity and smooth business operations.

Tencent Cloud closely monitors regulatory developments and publications from FSA and FISC and is committed to assisting financial institution customers in Japan in meeting compliance requirements. This document focuses on key regulatory guidelines of concern to financial institutions and explains how Tencent Cloud supports compliance with these requirements:

The Center for Financial Industry Information Systems (FISC):

- [FISC Security Guidelines on Computer Systems for Financial Institutions \(Thirteenth Edition\)](#)

The Financial Service Agency (FSA):

- [Payment Services Act \(PSA\)](#)
- [Guidelines on Cybersecurity for the Financial Sector](#)

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 life cycle 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)	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

in Japan

financial industry	obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure.
IT compliance audit in Thailand financial industry	Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange 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.
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	
	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 FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition)

The FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition) was issued by The Center for Financial Industry Information Systems (FISC) on March 21, 2025, with the aim of providing guidance for financial institutions and related entities to follow a risk-oriented approach and implement security measures. This publication systematizes security guidelines into four categories: control standards, practice standards, facility standards, and audit standards. Each category corresponds to different management objectives and application scenarios: the control standards cover the requirements for establishing the information technology governance and management system; the practice standards focus on improving the reliability and security of financial information systems; the facility standards aim to protect buildings and facilities where computer systems are located from threats such as natural disasters and illegal activities; the audit standards specify the audit requirements for the control standards, practice standards, facility standards, and related measures.

In this section, Tencent Cloud summarizes the requirements in The FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition) that are relevant to cloud service providers and explains how Tencent Cloud, as a CSP, assists financial institutions in complying with these requirements.

5.1 Control Standards

The control standards in The FISC Security Guidelines on Computer Systems for Financial Institutions (Thirteenth Edition) mainly include management system established for implementing information technology governance, as well as monitoring activities carried out to confirm whether the established management system is correctly applied and effectively functioning. The control standards are further divided into internal controls for internal management of the organization and external controls for managing other organizations such as outsourcing parties.

5.1.1 Internal Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
C1	Policy/Plan	[Basic] Establish regulations that define important matters pertaining to system security measures.	Customers should formulate basic policies, regulations, procedures and business processes related to system security and cybersecurity, to clarify the organizational structure, responsibilities of relevant parties, and matters that need to be managed for the proper implementation of security measures. Customers should also revise formulated policies, regulations, procedures, and processes as needed.
C1-1	Policy/Plan	[Basic] Establish a basic policy regarding cybersecurity measures.	
C1-2	Policy/Plan	[Basic] Establish regulations, procedures, and business processes regarding cybersecurity measures.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 has established a dedicated security governance framework, defining roles and responsibilities across different levels. 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. Tencent Cloud is certified against internationally recognized standards, including: • ISO/IEC 27001 – Information Security Management System. • ISO/IEC 27017 – Cloud Service Information Security Management. • ISO/IEC 22301 – Business Continuity Management. • ISO/IEC 20000 – IT Service Management.
C4	Organizational structure	[Basic] Establish a security management system.	Customers should establish a security management system to clarify management requirements for personnel, organization,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			scope of responsibilities, and authority. To support customers in meeting regulatory requirements, Tencent Cloud has established a dedicated security governance framework, defining roles and responsibilities across different levels and setting mechanisms for security audits and risk assessments. Tencent has formed a Security Technology Committee and specialized security teams across various domains. Additionally, Tencent Cloud maintains robust HR management standards and procedures to ensure personnel are recruited and assigned according to role requirements. Tencent Cloud brings together industry-leading security experts to deliver secure, reliable, professional, and compliant products and services. Regional Information Security Liaisons are appointed to maintain smooth communication with local regulators and customers, ensuring compliance with legislative, regulatory, and contractual obligations.
C4-1	Organizational structure	[Basic] Formulate a plan regarding management resources and personnel for managing cybersecurity.	Customers should allocate the necessary resources for managing cybersecurity in a reasonable manner and develop plans to allocate, cultivate, and manage cybersecurity personnel. To support customers in meeting regulatory requirements, Tencent has formed a Security Technology Committee and specialized security teams across various domains. Additionally, Tencent Cloud maintains robust HR management standards and procedures to ensure personnel are recruited and assigned according to role requirements. In terms of training and education, Tencent Cloud has implemented a

No.	Domain	Summary of Controls	Tencent Cloud's Response
			comprehensive Information Security Training Framework, which requires all formal employees, consultants, interns, and outsourced staff to complete information security training courses. These courses include mandatory training for all staff, specialized training for key roles, and optional professional courses. The training content covers areas such as basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.
			Customers should develop a management procedure for the entire lifecycle of information assets, classify and manage information assets based on their importance, use tools such as ledgers to manage information assets, and update information asset records in a timely manner.
C5-1	Organizational structure	[Basic] Properly manage information assets to identify cybersecurity risks.	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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			(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 complying with control principles, 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.
C5-2	Organizational structure	[Basic] Identify and assess cybersecurity risks, then formulate a risk response plan.	Customers should collect and analyze related information about threats and vulnerabilities, identify risks related to cybersecurity, assess the impact of risks, develop risk response plans, and monitor the effectiveness of risk control measures. Tencent Cloud provides Cloud Security Center (CSC) to support customers in risk management. As Tencent Cloud's unified security management platform, CSC can periodically detect six major risks—port, vulnerability, weak password, content, cloud resource configuration, and service exposure—and categorizes them for management. By aggregating logs from Cloud Firewall, WAF, and CWPP, CSC can

No.	Domain	Summary of Controls	Tencent Cloud's Response
			also analyze and consolidate alerts for unified display and handling. Additionally, Tencent Cloud provides the <u>Threat Intelligence Center (TIX)</u>, 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. To support customers in meeting regulatory requirements, Tencent Cloud has defined 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. Tencent Cloud conducts risk assessments regularly, 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.
C5-3	Organizational structure	[Basic] Establish procedures for vulnerability management of hardware, software, and other	Customers should develop relevant procedures for vulnerability management of hardware, software, and other

No.	Domain	Summary of Controls	Tencent Cloud's Response
		components. For high-severity vulnerabilities, it is desirable to manage vulnerability responses for systems owned by third parties, including cloud service providers. In managing such responses, financial institutions could consider using third-party assurance reports and contractual agreements.	components. According to these procedures, customers should take timely response measures based on the importance of the system, the risk level, and the severity of the system when vulnerabilities are discovered. Customers can use Cloud Workload Protection Platform (CWPP) to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, receive real-time alerts, and obtain remediation plans to quickly address vulnerability risks. Tencent Cloud Container Security Service (TCSS) provides a virtual patching system designed to protect against frequently occurring zero-day vulnerabilities. It integrates Tencent's vulnerability discovery and real-time high-risk vulnerability alerting technologies to capture and analyse vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically apply them to cloud servers to effectively block hacking attempts. In addition, customers can use Vulnerability Scanning Service (VSS) to perform regular security scans on enterprise network devices and application services, receive continuous risk alerts and vulnerability detection, and obtain professional remediation recommendations to reduce security risks. To support customers in meeting regulatory requirements, Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform. Tencent Cloud uses a vulnerability scanning system to perform regular scans for security vulnerabilities. The scanning scope covers the virtualization layer, system layer, and application layer. Upon completion of the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			scanning, the Tencent Cloud security team will analyze, categorize, and address the discovered vulnerabilities. Any identified security vulnerabilities are logged into the ticketing system to ensure they are properly handled within the stipulated timeframe. Tencent Cloud uses host endpoint detection tools to regularly scan patch installation status and records overdue patch installations in the ticketing system. In addition, Tencent Cloud undergoes regular independent third-party professional audits and publishes assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status. To request any relevant compliance certificates or reports, please submit a request through the Compliance Document Download for download. Tencent Cloud offers online legal documents on its international portal such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope and service levels of the offerings, and 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.
C5-4	Organizational structure	[Basic] Conduct cybersecurity exercises and training.	Customers should regularly conduct cybersecurity exercises and training to verify the effectiveness of their response procedure and emergency plans against cyber-attacks. Customers should also continuously improve their cybersecurity

No.	Domain	Summary of Controls	Tencent Cloud's Response
			exercises and training. Customers can leverage the Cloud Advisor (TSA) service to assist with planning and executing business continuity tests. This service is a cloud governance platform that integrates multiple ITOM vertical applications and draws on Tencent Cloud's extensive operational expertise. Through risk inspections, fault drills, and other governance measures, Cloud Advisor optimizes cloud infrastructure. It provides fault injection scenarios across IaaS and PaaS layers, as well as industry-specific drill templates covering typical use cases such as cross-availability zone disaster recovery. This helps customers quickly and efficiently reuse proven solutions based on their business needs, improving system availability. Tencent Cloud also provides Penetration Testing Service (PTS), which simulates real business scenarios with massive user traffic to comprehensively validate system availability and stability. To support customers in meeting regulatory requirements, Tencent Cloud regularly conducts cybersecurity training and drills. The drills typically simulate real-world disaster scenarios, including attack-defense exercises and large-scale failures, to thoroughly assess system resilience, response speed, and recovery capability, which ensure that business can quickly return to normal in case of emergencies. Tencent Cloud implements safeguards to prevent adverse impacts on services during drills. After each drill, relevant departments prepare a detailed drill report, and implement corrective actions based on the improvement measures outlined in the drill summary report.

No.	Domain	Summary of Controls	Tencent Cloud's Response
C5-5	Organizational structure	[Basic] Conduct education and training on cybersecurity.	Customers should conduct cybersecurity education and training to enhance personnel's awareness based on their roles and responsibilities, and to improve the knowledge and skills necessary for personnel to fulfill their job duties and respond to incidents. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.
C8	Organizational structure	[Basic] Establish a network management system.	To ensure proper and efficient operation of computer networks and to prevent unauthorized access, customers should define network management procedures and establish a formal management system. To assist customers in effectively managing network security, Tencent Cloud provides multiple services: • <u>Virtual Private Cloud (VPC)</u>: Uses tunneling technology to create virtual networks on physical infrastructure, achieving complete logical isolation between VPCs. Security groups and network ACL rules enable granular control of inbound and outbound traffic at both instance and subnet levels. • <u>Cloud Firewall (CFW)</u>: Offers ACL-based firewall control, IPS real-time interception, virtual patching, and malicious code detection to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			protect network boundaries.
			• <u>Web Application Firewall (WAF)</u>: Defends against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and malicious crawlers. • <u>Anti-DDoS</u>: Combines abundant, high-quality DDoS mitigation resources with evolving proprietary and AI-driven detection algorithms to counter DDoS attacks. • <u>Flow Logs (FL)</u>: Provides real-time, non-intrusive traffic collection, storage, and analysis to support troubleshooting, architecture optimization, security detection, and compliance auditing.
			Tencent Cloud establishes a network security management standard and a layered defense system. Through policies and processes, Tencent Cloud defines security controls, protection standards, and corresponding roles and responsibilities to ensure secure network operations. Tencent Cloud deploys a mature security architecture incorporating firewalls, IDS/IPS, DDoS protection, network isolation, and web security mechanisms to detect, filter, and block malicious traffic. Regarding the management of network devices, Tencent Cloud operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls, and servers, and uses a ticketing system to track and resolve identified security issues. The production environment is fully equipped with bastion hosts, which centrally manage account permissions for network devices and strictly prohibit

No.	Domain	Summary of Controls	Tencent Cloud's Response
			unauthorized access to internal network resources. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to 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.
C10	Organizational structure	[Basic] Establish and maintain an organization for disaster prevention.	To prevent disasters and minimize damage, customers should establish a disaster emergency organization and clarify relevant responsible personnel. To support customers in meeting regulatory requirements, Tencent Cloud has established emergency response procedures and defined the roles and responsibilities of personnel in the business recovery processes. For key positions, Tencent Cloud adopts a personnel replacement mechanism and regularly conducts emergency drills and training to ensure that the recovery procedures can be executed quickly and effectively.
C11	Organizational structure	[Basic] Establish a proper crime prevention organization.	Customers should establish a proper crime prevention organization to prevent unauthorized entry, bringing in hazardous materials, illegal removal of assets, and other acts threatening the security of computer systems, as well to respond rapidly in case a crime occurs and minimize its impact. For physical environment security, Tencent Cloud has implemented physical security management policies to standardize operational safety, promptly identify risks, and strengthen physical security controls. In Japan, Tencent Cloud operates two leased data centers. To ensure resilience and security, Tencent Cloud has established a rigorous management system

No.	Domain	Summary of Controls	Tencent Cloud's Response
			covering supplier onboarding, contractual obligations, and continuous oversight. For physical access control, Tencent Cloud requires operators to implement formal access procedures, verify personnel identity, and inspect and register carried items. Operators must also implement approval and inspection processes for equipment entering or leaving server rooms (e.g., installation, decommissioning, or relocation). For security and monitoring, Tencent Cloud requires operators to conduct daily inspections of server rooms and equipment according to predefined checklists and schedules, recording signatures and timestamps at each checkpoint. Operators must immediately activate emergency response procedures upon detecting infrastructure failures or security incidents. Data centers must be equipped with 24/7 video surveillance systems with no blind spots, monitored from a security control room, and ensure secure retention of surveillance records for an adequate duration.
C14	Personnel (Staffing/Training)	[Basic] Carry out security training.	Customers should disseminate the security policy within the organization and conduct security training tailored to the specific duties of all staff. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Framework, which requires all formal employees, consultants, interns, and outsourced staff to complete information security training courses. These courses include mandatory training for all staff, specialized training for key roles, and optional professional courses. The training content covers areas such as

No.	Domain	Summary of Controls	Tencent Cloud's Response
			basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.
			Customers should implement education and training based on the duties and responsibilities of staff to improve their knowledge and skills related to the system and the business they are responsible for. To enhance customers' technical capabilities and cloud proficiency, Tencent Cloud offers Tencent Cloud Training and Certification based on product knowledge and relevant professional expertise, and provides materials such as the operation processes and user manual of cloud services through the official website. To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive training mechanism and set up diversified career development paths. Tencent Cloud provides staff with abundant and high-quality learning resources, and continuously optimizes the training system to ensure that the staff have necessary skills and qualifications for their responsibilities, while also supporting their personal growth and career development.
C15	Personnel (Staffing/Training)	[Basic] Carry out education to improve skills of personnel.	
			Customers should provide education and training on computer system operations related to system failures and disasters. To support customers in meeting regulatory requirements, Tencent Cloud's related departments periodically conduct scenario-based training and drills for security incident response plans. Tencent Cloud also provides ongoing technical training for its security teams based on evolving technologies and threat landscapes,
C16	Personnel (Staffing/Training)	[Basic] Provide proper education and training for possible failures and disasters.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			ensuring staff understand and comply with the latest security standards and best practices and can respond quickly and effectively to security incidents.
C18	Personnel (Staffing/Training)	[Basic] Implement proper personnel management for staff.	Customers should implement appropriate personnel management strategies to manage staffing, rotation, and other personnel related matters. To support customers in meeting regulatory requirements, Tencent Cloud has formed professional teams for different fields and established comprehensive human resource management standards and procedures to ensure that personnel are selected, recruited, and arranged according to job requirements. Tencent Cloud gathers teams of experts dedicated to providing customers with reliable, professional, and compliant products and services.

5.1.2 External Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
C20	Outsourcing management	[Basic] When outsourcing, identify the purpose and scope beforehand and clearly define the procedures for selecting contractors. It is necessary to objectively evaluate outsourcing providers. It is desirable to continuously evaluate outsourcing providers throughout the contract period.	When customers implement outsourced commissions, they should assess the division of responsibilities between themselves and the outsourcing providers based on an understanding of the scope of the outsourced task and the nature and usage model of the provider's service. Customers should also evaluate the provider's qualifications, operational capability, internal controls, and risk management status. Furthermore, Customers should continuously evaluate the outsourcing providers within the period of contract. If all or part of an outsourced task will be further subcontracted (re-outsourced), the customers must evaluate the subcontractor(s) based on its content and risk characteristics to verify the appropriateness of their selection by the primary provider.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			In terms of responsibility distinction, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement on its international portal. These documents clearly define the scope and service levels of the offerings, as well as 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. Considering that control responsibilities vary across service models (IaaS, PaaS, SaaS), Tencent Cloud has established a Shared Responsibility Model, detailed in Section 3 “Tencent Cloud Security Responsibility Sharing Model”. Regarding the evaluation of outsourcing providers, 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: • Resources and Scale : Tencent Cloud's operational capabilities and scale are among the leaders in the industry. Its data centers are deployed across multiple global regions, covering Mainland China, the Asia-Pacific region, North America, and Europe. • 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. Business Continuity and Disaster Recovery: Tencent Cloud has obtained ISO/IEC 22301 certification for its Business Continuity Management System. To ensure the continuous availability of customer services, Tencent Cloud has developed detailed disaster recovery plans for its cloud products and conducts regular drills in strict accordance with requirements to ensure the timeliness and feasibility of these plans. Data Security: Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data content. Adhering to the principle of "data privacy," Tencent Cloud employs multi-layered technical isolation measures to ensure data segregation and prevent tenants from accessing, obtaining, or tampering with other tenants' data. Tencent Cloud's storage and database products support data encryption by using secure algorithms to ensure data confidentiality. Risk Management: Tencent Cloud develops and maintains an internal risk management framework based on the ISO/IEC 27001:2022 standard to identify, analyze, and manage recognized risks. Tencent Cloud conducts a formal risk assessment at least annually, referencing sources such as industry security incident reports, Tencent Cloud's accumulated practices, and professional risk databases.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Risks within Tencent Cloud's products and service processes are identified and evaluated based on asset value, likelihood, and impact severity, resulting in a calculated risk level. Based on the risk analysis, Tencent Cloud formulates mitigation strategies and implements corresponding measures to reduce risks to an acceptable level. • Subcontract Management: Tencent Cloud publishes the online Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, and other legal documents on its international portal. For sub-processing scenarios, these agreements expressly set out clauses on prior consent to sub-processing, advance notice of any addition or replacement of sub-processors, and data-protection obligations. Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the relevant contract/agreement without the customer's prior written consent. Any anticipated change involving the addition or replacement of a sub-processor will be notified to the customer by e-mail or other agreed channels. Customers may also elect to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Regarding sub-contractor management, Tencent Cloud maintains a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers. • Audit and Evaluation: Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			undergoes regular independent third-party professional audits and publishes assurance-based reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status for service organizations. For the Japanese region, Tencent Cloud evaluated the current control status according to the "FISC Security Guidelines on Computer Systems for Financial Institutions" and prepared corresponding System and Organizational Control (SOC) reports on this basis. In addition, Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. • Support Mechanism: Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of cloud services and provides real-time monitoring through the management console. Additionally, Tencent Cloud offers a ticketing service via the Tencent Cloud console, allowing customers to report faults, incidents, problems, and complaints related to security, availability, and confidentiality. Customers may also choose applicable service plans to access dedicated support groups, a designated technical account manager, and value-added services as part of a tailored support offering.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• Notification Mechanism: Tencent Cloud provides multiple communication channels, including the console, official website, and email, to fulfill notification and communication obligations. 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 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. • Termination of Contract: 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. 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.
C21	Outsourcing management	[Basic] Conclude proper contracts with the contractor, including provisions on security measures. “Considerations for Cloud Usage”: • For service discontinuation initiated by the cloud provider, confirm in advance the required notice period, considering: criticality of the business using	Customers should sign contracts with outsourcing providers that include security measures, confidentiality protection, and smooth system operation. Customers should reach agreement with the provider on the service level through methods such as signing Service Level Agreements (SLAs). As a cloud service provider, Tencent Cloud offers online legal documents on its international portal such as the Terms of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the cloud service; cost and human effort required for system reconstruction. - It may be difficult for financial institutions to conduct prior reviews of cloud providers' subcontractors. Instead, require the cloud provider (via contract) to disclose: scope of outsourced services; security measures and implementation status at subcontractor level. Alternatively, verify through third-party attestation reports. - Direct audits by financial institutions may be impractical. Consider using third-party attestation reports (e.g., SOC reports) as an alternative. - On-site investigation may not be feasible within the cloud provider's infrastructure. As an alternative, confirm in advance whether the provider can issue a detailed incident report when significant impacts occur. - Some cloud providers do not issue deletion certificates. In such cases, verify deletion practices through third-party attestation reports.	<u>Service, Service Level Agreement (SLA)</u>, and <u>Data Processing and Security Agreement</u>. 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, the service term, and the scenarios under which the agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. For sub-contracting scenarios, Tencent Cloud publishes the online <u>Terms of Service</u>, <u>Service Level Agreement (SLA)</u>, <u>Data Processing and Security Agreement</u>, and other legal documents on its international portal. These agreements expressly set out clauses on prior consent to sub-processing, advance notice of any addition or replacement of sub-processors, and data-protection obligations. Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the relevant contract/agreement without the customer's prior written consent. Any anticipated change involving the addition or replacement of a sub-processor will be notified to the customer by e-mail or other agreed channels. Regarding sub-contractor management, Tencent Cloud maintains a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic

No.	Domain	Summary of Controls	Tencent Cloud's Response
			monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers. In terms of auditing, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture and ensure compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes regular independent third-party professional audits and provides assurance reports on system and organizational controls to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud services. For the Japanese region, Tencent Cloud evaluated the current control status according to the "FISC Security Guidelines on Computer Systems for Financial Institutions" and prepared corresponding System and Organizational Control (SOC) reports on this basis. In addition, Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. In terms of event reporting and notification, Tencent Cloud has implemented an Information Security Incident Communication and Early Warning Management Procedure, establishing clear warning and notification mechanisms for significant security incidents and major business disruption scenarios, and promptly inform and alert affected internal personnel, customers, and other relevant parties, ensuring orderly, timely, and efficient communication and coordination.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels and provide technical support to help minimize losses. In terms of data deletion, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data—including replicas and backups—after the retention period. Deleted data cannot be restored.
C22	Outsourcing management	[Basic] Ensure that the contractor's staff comply with the rules and check their state of compliance. In the case of cloud services, unlike general outsourcing, it may be difficult for financial institutions to require cloud providers to directly comply with all institution-defined rules. Therefore, financial institutions must assess whether the security measures implemented and disclosed by the cloud provider (e.g., via public documentation or certifications) are acceptable from a risk and compliance standpoint. When conducting such assessments, the use of third-party attestation reports (e.g., SOC 1/2, ISO 27001 certification) is recommended.	Customers should require outsourcing provider personnel to comply with their various policies and rules based on the content and scope of the outsourcing business, and confirm the outsourcing provider's compliance through measures such as auditing or receiving regular reports from the outsourcing provider. Customers should also limit the access permissions granted to outsourced provider personnel to the minimum extent necessary to perform their business. To facilitate the Customer's audit and review requirements, Tencent Cloud will provide dedicated assistance and actively cooperate with Customer-initiated audit or review activities. Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes regular independent third-party audits and assessments. Through these audits, Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications. Based on Customer requirements, Tencent Cloud provides assurance reports on system and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			organizational controls to cloud users, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud services. For the Japanese region, Tencent Cloud evaluated the current control status according to the "FISC Security Guidelines on Computer Systems for Financial Institutions" and prepared corresponding System and Organizational Control (SOC) reports on this basis, covering control points related to the security, availability, and confidentiality of the Tencent Cloud platform. 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.
C23	Outsourcing management	[Basic] Establish a management structure for outsourcing and check the state of the performance of outsourced tasks. In the case of cloud services, it may be difficult to apply the same operational monitoring methods used for traditional outsourcing. Therefore, financial institutions must assess, based on publicly available information from the cloud provider, whether the implemented security measures, their compliance status, and service availability records are acceptable from a risk management standpoint. Third-party attestation reports (e.g., SOC reports, ISO certifications) may be used for such assessments.	Customers should establish an outsourcing management system and check the execution of outsourcing business based on outsourcing contracts and agreements. Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of cloud services and provides real-time monitoring through the management console. In addition, Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. To support customers' outsourcing management requirements, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			provides the Tencent Cloud's Observability Platform (TCOP), which enables real-time monitoring, analysis, and alerting for cloud products and resources. TCOP collects monitoring metrics reported by Tencent Cloud services and customer-defined configurations, presenting them through visual dashboards to help customers track the operational status and performance of cloud products. It also supports alert configuration based on defined thresholds and sends notifications via message push and other channels to promptly inform customers of business anomalies. Additionally, 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. 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.
C24	Use of cloud services	[Basic] When using a cloud service, set up security measures with cloud service-specific risks considered. 1. When using cloud services for Critical Systems, financial institutions must pay attention to applicable domestic and international laws, regulations, and evaluation frameworks during provider selection and throughout the service lifecycle. They must also identify the Controlled Cloud Locations (a Controlled Cloud Location refers to any site through which effective access to data is possible, considering the wide-area nature of cloud	Customers should take security measures to address the cloud service-specific risks when using a cloud service. Customers should pay attention to domestic and foreign laws when using a cloud service, and set cloud nodes and data storage locations in countries or regions that can implement substantive control. To support customers in meeting regulatory requirements, Tencent Cloud's infrastructure is deployed across multiple global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an isolated fault domain with physical separation. Customers can flexibly deploy data and systems across different regions or

No.	Domain	Summary of Controls	Tencent Cloud's Response
		computing) and the countries or regions where data is stored. These locations must be in jurisdictions where effective control can be carried out. For General Systems, these measures should be implemented according to the service content and risk profile.	availability zones based on business growth needs and data security requirements to meet disaster recovery objectives. Currently, Tencent Cloud operates two data centers in Japan, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Japan-based Customers may choose to store and process their data locally within Japan. Tencent Cloud strictly complies with the laws and regulations of the jurisdictions in which it operates and has established security and compliance programs to ensure that information security operations meet applicable legal, regulatory, and industry standards. Tencent Cloud adheres to principles of transparency. Upon request, Tencent Cloud will promptly provide information through appropriate channels regarding data storage locations and backup storage locations.
		2. For Critical Systems, financial institutions must explicitly include necessary rights (e.g., audit rights) in contracts or agreements with cloud providers to ensure enforceable control over Controlled Cloud Locations. For General Systems, implementation should be risk-based.	Customers should conduct audits and monitoring of cloud service providers through methods such as using third-party assurance reports when using cloud services. Customers should clearly record this right in contracts or other documents signed with cloud service providers.
		3. Security measures implemented by the cloud provider within their responsibility scope should generally be managed in accordance with control standards, with reference to practical guidelines. However, due to limitations in direct control, financial institutions may use third-party attestation reports (e.g., SOC, ISO) as an alternative.	As a cloud service provider, Tencent Cloud offers online legal documents on its international portal 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, the service term, and the scenarios under which the
		4. For audits, it is desirable to use	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		assurance-type audit reports (or equivalent) issued by the cloud provider, considering technological complexity and advancements. Third-party attestation reports can also be used not only for audits but also to confirm rule compliance and operational status of cloud provider personnel.	agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. To support customers' outsourcing oversight requirements, Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. Tencent Cloud also undergoes regular independent third-party professional audits and publishes assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status for service organizations.
		5. For Critical Systems, regular audits of cloud providers must be conducted. For General Systems, regular audits are recommended.	
		6. For Critical Systems, financial institutions must assign personnel with specialized technical knowledge (e.g., cloud technologies) to effectively conduct audits and monitoring of cloud providers. For General Systems, such staffing is recommended. If internal acquisition or training is difficult, this requirement may be fulfilled through third-party auditors with relevant expertise.	For the Japanese region, Tencent Cloud evaluated the current control status according to the "FISC Security Guidelines on Computer Systems for Financial Institutions" and prepared corresponding System and Organizational Control (SOC) reports on this basis, covering control points related to the security, availability, and confidentiality of the Tencent Cloud platform.
		7. As cloud service technologies evolve, service models and usage patterns may change. Therefore, financial institutions must consider various cloud models (e.g., IaaS, PaaS, SaaS) from the outset and clearly define the responsibility boundary between themselves and the cloud provider before commencing service use.	Customers should clarify their responsibilities with cloud service providers based on different models of cloud services. Tencent Cloud adheres to the principles of openness and sharing in cloud computing services, continuously enhancing the security capabilities of its cloud platform and services. Together with customers, we strive to build a more comprehensive and robust security assurance system for cloud-based business and data. As a cloud service provider, Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Recognizing that customers' level of control

No.	Domain	Summary of Controls	Tencent Cloud's Response
			varies depending on the type of cloud service selected (such as IaaS, PaaS, and SaaS), Tencent Cloud has established a Shared Responsibility Model for Cloud Security based on different service categories. For details, please refer to Section 3: "Tencent Cloud Security Responsibility Sharing Model."
		8. Data stored in the cloud may be exposed due to changes in access permission specifications or misconfigurations by the financial institution. Therefore, for Critical Systems, financial institutions must confirm that the cloud provider will notify them in advance of any changes to access permission settings. Additionally, whenever access permission specifications or institutional configurations are changed, the validity of the settings must be verified. This verification may be supported by: expert system audits; automated misconfiguration detection services (e.g., CSPM – Cloud Security Posture Management); cloud provider-recommended architectural principles and best practices. For General Systems, these measures should be applied based on service content and risk characteristics.	Customers should ensure that the cloud service provider will notify before any changes are made to the access permission settings. Customers should check the reasonableness of the configuration when setting access permissions or making internal configuration changes within the organization. To support customers in configuring cloud resource permissions, Tencent Cloud provides Cloud Access Management (CAM). CAM can help users to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. Tencent Cloud also provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions. Additionally, user guides and operating procedures for cloud products such as CAM and BH have been documented and provided to customers through Tencent Cloud official websites. Customers can refer to relevant guidance for permission configuration. To promptly identify configuration errors, Tencent Cloud provides Cloud Security Center (CSC). The 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,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			continuously recording configuration details and changes across different regions under their account. Based on Tencent Cloud best practices and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. 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. In terms of authorization management, Tencent Cloud also implements authorization policies and a privilege separation matrix, maintaining records of personnel identity information mapped to job roles and corresponding permission levels for each business system. Regular internal permission reviews are conducted to prevent misuse or abuse of access rights. Any unnecessary access rights are promptly revoked. Furthermore, customer data is classified as high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents).
C28	Cybersecurity risk management	[Basic] Appropriately manage cybersecurity risks across the supply chain.	Customers shall formulate a cybersecurity strategy covering the entire supply chain and establish a cybersecurity management

No.	Domain	Summary of Controls	Tencent Cloud's Response
			mechanism that encompasses all business processes. Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of cloud services and provides real-time monitoring through the management console. customers can also 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. Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. Tencent Cloud also undergoes regular independent third-party professional audits and publishes assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status for service organizations. In terms of subcontractor management,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud has established a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers. Tencent Cloud enters into formal service agreements with its subcontractors that explicitly set out responsibilities and obligations relating to security, privacy protection, confidentiality, and compliance. In addition, Tencent Cloud continuously monitors subcontractors' service levels to ensure that sub-processing operations remain secure and stable. In accordance with the security and operational standards stipulated in the contracts, Tencent Cloud regularly assesses subcontractors' delivery performance and takes appropriate remedial action for any issues identified, thereby ensuring that their deliveries meet the agreed security and quality requirements.

5.2 Practice Standards

5.2.1 Information Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
P1	Data protection	[Basic] Take measures to prevent others from finding out personal identification numbers (PINs) and passwords. In the case of cloud services, it is necessary to verify whether the cloud service provider meets the security standards established by financial institutions. The verification points include: (1) measures implemented by the cloud provider to prevent leakage of PINs and passwords for	Customers should take measures to prevent the leakage of PINs and passwords. When using cloud services, customers should confirm that the password/ PINs anti-leakage measures implemented by the cloud service provider meet the security standards. To support customers in meeting regulatory requirements, Tencent Cloud has established access control procedures that define standards for setting and protecting account passwords of cloud customers. Each user is assigned a unique account

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management interfaces used by financial institutions; (2) password restrictions imposed by the cloud service specifications (e.g., length, allowed character types). Financial institutions must examine leakage prevention measures based on the above verification results and implement additional measures if any deficiencies are found.	identifier upon registration, and password policies are enforced. When logging into the console, identity credentials and operational commands are transmitted securely via HTTPS. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to encrypt passwords, avoiding plaintext storage. Tencent Cloud supports multi-factor authentication (MFA) to enhance the security of account logins and sensitive operations such as password changes. Password reset and modification functions are also available. Tencent Cloud provides a Cloud Access Management (CAM) service to help customers securely manage access to Tencent Cloud resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions. Through the CAM console, customers can configure password policies for sub-users. Tencent Cloud also sets password policies for employee accounts based on security baselines, including password length, complexity, locking, and resetting.
P3	Data protection	[Additional] Take measures for the protection of stored data against disclosure. In the case of cloud services, it is necessary to verify whether the cloud service provider meets the security standards established by financial institutions. Verification points include: (1) confirming the cloud provider's access rights to encryption keys; (2) verifying the scope and strength of encryption. Financial institutions must assess whether additional encryption	Customers should take data protection measures for important data to prevent data leakage caused by illegal copying or theft. When using cloud services, customers should check the encryption scope and strength of the cloud service provider, as well as the access permission management of the encryption key. To protect the confidentiality and integrity of customer data, Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption keys are managed through the integrated Key Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
		measures are needed based on the above verification results.	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. Invalid, expired, or compromised keys are securely deleted using reliable methods, and once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. To support customers in meeting regulatory requirements, Tencent Cloud has established encryption and key management standards that mandate the use of cryptographic algorithms during data transmission and storage. For key management, Tencent Cloud selects cryptographic products and algorithms that comply with international cryptographic policy requirements.
P4	Data protection	[Additional] Take measures to prevent leakage of transmission data. In the case of cloud services, it is necessary to verify with the cloud service provider the protective measures for important data during data transmission. Financial institutions must implement data protection measures for important data during data transmission based on the verification results.	Customers should take protective measures for the transmission of important data, such as encryption, to prevent data leakage caused by eavesdropping during the transmission process. When using cloud services, customers should check the protection measures during data transmission with the cloud service provider. 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: • Virtual Private Cloud (VPC): Uses tunneling technology to create virtual

No.	Domain	Summary of Controls	Tencent Cloud's Response
			networks on physical infrastructure, achieving complete logical isolation between VPCs. Security groups and network ACL rules enable granular control of inbound and outbound traffic at both instance and subnet levels. • <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. To support customers in meeting regulatory requirements, Tencent Cloud has developed data security baselines, specifying the secure data transmission protocols that need to be used and the prohibited insecure data transmission protocols to prevent data leakage during transmission.
P5	Data protection	[Basic] Provide the function of controlling access to files. In the case of cloud services, it is necessary to verify whether the access control functions provided by the cloud service provider meet the security standards established by financial institutions. Verification points include: (1) access control methods; (2) access control checking functionality; (3) scope of access. When financial institutions use cloud service	Customers should set up access control and permission checks for programs and files to prevent unauthorized access. When using cloud services, customers should check whether the access control functions provided by the cloud service provider meet security standards. Through the <u>Cloud Access Management (CAM)</u> console, Tencent Cloud provides customers with secure permission assignment and sub-user management capabilities. CAM enables customers to define which actions and resources each

No.	Domain	Summary of Controls	Tencent Cloud's Response
		functionalities for access management, they must design, implement, and operate access permission checking functions based on the above verification results.	user or role can access. Customers can also enable MFA for both primary and sub-accounts to enhance account security. CloudAudit provides comprehensive logging and continuous monitoring of user activities and API usage across Tencent Cloud infrastructure. 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. To support customers in meeting regulatory requirements, in terms of data access protection, Tencent Cloud has implemented access control management standards and established permission and authorization mechanisms. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions only when necessary and through a rigorous approval process. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities. Regular internal permission reviews are also conducted to prevent misuse or abuse of access rights. Any unnecessary access rights are promptly revoked. Furthermore, Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Internal

No.	Domain	Summary of Controls	Tencent Cloud's Response
			operations personnel must obtain approval before accessing bastion hosts, and authorized personnel must complete secondary identity verification to log in. All backend operation records are stored centrally on a logging platform and reviewed periodically by Tencent Cloud's internal audit team.
			Customers should take tamper detection measures during the transmission of important 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. Tencent Cloud has developed data security baselines, specifying the secure data transmission protocols that need to be used and the prohibited insecure data transmission protocols. Customers can further enhance data transmission security using the following services: • <u>Cloud Connect Network (CCN):</u> CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal path selection, and fast failover capabilities. All communication within CCN remains off the public internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link
P7	Data protection	[Additional] Take measures for the detection of tampered transmitting data. In the case of cloud services, it is necessary to confirm with the cloud service provider what tamper prevention measures are implemented within the portion of the transmission path under the cloud provider's control. It is desirable for financial institutions to implement tamper detection measures for data transmitted between their own systems (including on-premises environments) and cloud data centers.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			redundancy further enhances communication reliability, making data transmission secure and dependable. • <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.
P8	Prevention of unauthorized use	[Basic] Set up functions of personal identification. In the case of cloud services, it is necessary to confirm with the cloud service provider the identity verification functions implemented for unique management objects within the cloud service. Multi-factor authentication is desirable. Financial institutions must configure identity verification functions for the management objects confirmed above.	Customers should check the legitimacy of the connecting party based on the business content and connection method. When using cloud services, customers should confirm with the cloud service provider the authentication functions implemented in the cloud service management objects (such as management interfaces). Tencent Cloud provides <u>Cloud Access Management (CAM)</u> to help customers securely and granularly manage access to Tencent Cloud products and resources. CAM supports multiple methods of secondary identity verification, including MFA device validation or SMS verification codes, to ensure identity and environment security before login and sensitive operations. Tencent Cloud provides <u>Bastion Host (BH)</u> to assist customers in user management, authorization management, and comprehensive auditing. BH provides differentiated authentication methods

No.	Domain	Summary of Controls	Tencent Cloud's Response
			according to different needs. It supports the basic static password method and can integrate existing authentication methods (such as LDAP). It also supports two-factor authentication for higher security and unified authentication management. To support customers in meeting regulatory requirements, Tencent Cloud has established internal access control management standards requiring user accounts to use unique identifiers and enforcing password policies for employee accounts based on security baselines. Tencent Cloud uses a Zero Trust security management system to authenticate employee access; users must complete multi-factor authentication before accessing internal resources. Additionally, Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before accessing bastion hosts, and authorized personnel must complete secondary identity verification to log in.
p9	Prevention of unauthorized use	[Basic] Provide the function of preventing unauthorized use of IDs. In the case of cloud services, it is necessary to confirm with the cloud service provider the unique IDs used within the cloud service. Examples of such unique IDs include administrative accounts provided by the cloud provider. Financial institutions must implement unauthorized use prevention measures for the IDs confirmed above.	Customers should take measures to prevent IDs used to access systems and data from being illegally used. When using cloud services, customers should confirm their IDs with the cloud service provider and take measures to prevent illegal use of the IDs. In terms of cloud-user access-control management, Tencent Cloud has established access control procedures that define standards for cloud customer account registration, management, and support. Customers are provided with access control features that enable them to define and enforce their own access policies

No.	Domain	Summary of Controls	Tencent Cloud's Response
			for managing the cloud services they have purchased. The management console serves as the central platform for customers to manage and control their cloud resources. Each customer is assigned a unique account identifier upon registration, and password policies are enforced. The console automatically verifies the uniqueness of account names. When logging into the console, identity credentials and operational commands are transmitted securely via HTTPS. Customers can also manage cloud services and data centrally through open APIs, which require authentication using access keys assigned to each customer. Tencent Cloud supports multi-factor authentication (MFA) to enhance the security of account logins and sensitive operations such as password changes. Password reset and modification functions are also available. To support customers in meeting regulatory requirements, Tencent Cloud has established internal access control standards that mandate the use of unique identifiers for user accounts and enforce password policies based on security baselines. Tencent Cloud has set login failure limits and session timeout policies for internal terminals, operating systems, applications, and network devices.
P10	Prevention of unauthorized use	[Basic] Manage access records. In the case of cloud services, it is necessary to verify with the cloud service provider how access logs for the management interface are managed. Financial institutions shall regularly review the access logs of the management interface based on the above confirmation to	Customers should collect access logs of systems and data, retain such logs as audit evidence for the requisite period, and perform periodic reviews thereof. Where cloud services are utilized, the Customer shall verify with the cloud service provider the following details in respect of the access logs of its management interface: log content, log retention period, log protection measures, log provision methods and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		verify the legitimacy of access. In the case of cloud services, it is desirable to verify the time zone used by the cloud service provider. Financial institutions should pay attention to any time zone differences between their own systems and the cloud system that could cause time discrepancies. Additionally, when using cloud systems across multiple regions, be aware that multiple time zones may be involved.	timelines, and the time zone employed by the cloud service provider; the Customer shall additionally conduct periodic reviews of access logs. Regarding the collection and retention of access and operation logs, customers can use CloudAudit 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 provides Cloud Log Service (CLS) for customers to assist with log management. CLS is a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. 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 terms of timestamps, Tencent Cloud displays the current accurate Coordinated Universal Time (UTC) via the Network Time Protocol (NTP). Tencent Cloud provides internal NTP servers for use by cloud instances. For non Tencent Cloud devices, customers can use the public NTP servers provided by Tencent Cloud. In addition, Tencent Cloud requires data center operators to regularly check the time synchronization status of their NTP servers. To support regulatory compliance, Tencent Cloud has established comprehensive log collection and management standards covering the recording, extraction, storage, protection, analysis, and au-diting of login

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
P13	Prevention of unauthorized use	[Additional] Provide a function that protects cryptographic keys on devices and media that store electronic encryption keys, or software included with them. In the case of cloud services, it is necessary to confirm the following aspects regarding the cryptographic key management services provided by the cloud service provider: Cryptographic keys must remain under the ownership of the financial institution, and the cloud provider must not have unauthorized access; appropriate authorization settings, access controls, and audit logging are in place for key usage. In the case of cloud services, financial institutions must design, implement, and operate cryptographic key management based on the following considerations: (1) grant key usage privileges only to a minimum necessary number of personnel, and use these privileges to configure authentication and access rights; (2) generate audit logs for all cryptographic key usage activities and properly preserve these logs.	Customers should set up key protection functions in devices, media, or software that store electronic cryptographic keys. When using cloud services, customers should verify with the cloud service provider the ownership, storage method, access management, and the operation and audit log of the keys. The key usage permissions should only be granted to the minimum necessary personnel, and all key usage activities should be logged and stored. Tencent Cloud provides Key Management Service (KMS) to assist customers in achieving full lifecycle management of cryptographic keys, ensuring that keys are generated, stored, distributed, imported, exported, used, recovered, archived, and destroyed in a secure manner to prevent key leakage. A CMK, as a core resource in KMS, is protected by a third-party certified hardware security module (HSM) and used as a first-level key for encryption and decryption. Users can use the automatic CMK generation feature in KMS or import your own key to generate a CMK. KMS uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect CMK. There are two types of CMKs: Customer Managed CMK and Tencent Cloud Managed CMK. The Customer Managed CMK is a CMK that users create in the console or through APIs. Users can create,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			enable, disable, rotate keys and manage permissions of their Customer Managed CMK. The Tencent Cloud Managed CMK is a CMK that is automatically created for users when a Tencent Cloud product/service (such as CBS, COS, or TDSQL) calls the KMS service. Users can query and rotate Tencent Cloud managed CMKs. The CloudAudit logs KMS operation events. Users can check event history by logging in to the CloudAudit console. Tencent Cloud has also established internal encryption and key management standards, defining security requirements for key application, generation, storage, usage, transmission, rotation, and destruction. All key lifecycle operations follow strict controls, including dual authorization, secure handover, proper storage, and timely updates. During key usage, Tencent Cloud enforces segregation of duties, rigorous approval processes, and real-name operations, while maintaining detailed key operation logs and performing regular audits.
P14	Set up functions for protection against unauthorized access from external network	[Basic] Take preventive measures against unauthorized access from external networks. In the case of cloud usage, financial institutions must confirm with the cloud service provider the intrusion prevention measures implemented within the cloud service, particularly those relevant to the financial institution's usage, and based on this, consider additional intrusion prevention measures on the financial institution's side. In the case of cloud usage,	Customers shall adopt appropriate measures to prevent unauthorized intrusions at the connection points between external networks (such as open networks and remote access networks) and internal networks. When using cloud computing services, customers shall confirm with the cloud service provider the unauthorized intrusion prevention measures implemented in the cloud services, and consider adding corresponding prevention measures on the financial institution's side based on the confirmation results. Customers shall also confirm with the cloud service provider the means for verifying access records and the specifications of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		financial institutions must confirm with the cloud provider the specifications of access history review mechanisms and access monitoring functions offered by the cloud service. Financial institutions must obtain and evaluate vulnerability information published by cloud providers and consider appropriate responses.	access monitoring functions provided by the cloud services. To implement network perimeter protection, 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. 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. Customers can also 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			instance and subnet levels, enabling multi-layered network access control. For internal network security protection and management, Tencent Cloud has established network security management specifications and a network defense-in-depth system. Tencent Cloud has defined network security control and protection standards as well as corresponding roles and responsibilities through management systems and processes, ensuring the secure operation of businesses hosted on Tencent Cloud's network. Meanwhile, Tencent Cloud designs its network security architecture with reference to industry best practices, divides security domains based on business functions and security risks, implements physical or logical isolation for different security domains, and ensures the security of office networks and production networks through access control, boundary protection and other measures. Tencent Cloud adopts multiple protection mechanisms such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, and web security protection to detect, filter and block malicious network traffic in a timely manner, thereby protecting Tencent Cloud's network security. For log management, <u>Cloud Firewall (CFW)</u> 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. Customers can also use <u>Cloud Log Service (CLS)</u>, a one-stop log service platform that provides a range of services from log collection, log storage to log search and analysis, real-time consumption, and log delivery. It helps

No.	Domain	Summary of Controls	Tencent Cloud's Response
			customers address issues related to business operation, security monitoring, log auditing, and log analysis. In addition, <u>Cloud Security Center (CSC)</u> uniformly collects various types of cloud security-related data, including alert data from cloud security products, cloud asset configuration change data, operation behavior data of cloud users, and log data from some cloud products. It also provides a unified search and investigation platform to help customers achieve comprehensive cloud-based log auditing, search and investigation. 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. Regarding vulnerability disclosure, after confirming the existence of a vulnerability, Tencent Cloud will assess the impact of the vulnerability on customers' businesses and promptly notify customers of relevant vulnerability information via official website announcements and in-site messages following internal team review. The notification content includes but is not limited to an overview of the vulnerability, scope and degree of impact, control measures already taken by Tencent Cloud, repair suggestions proposed for customers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and specific operation guidelines.
P14-1	Set up functions for protection against unauthorized access from external network	[Basic] Implement Monitoring and Analysis Measures to Detect Early Signs of Cyberattacks.	Customers shall formulate procedures related to monitoring, analysis, and reporting, and take necessary monitoring and analysis measures to detect attacks based on the level of cyberattack threats. They shall also conduct continuous monitoring of access to and abnormal activities within data centers and server rooms. Customers can leverage Cloud Security Center (CSC) to achieve a closed-loop security operation cycle covering pre-attack threat detection, in-attack response and handling, and post-attack traceability analysis through its core modules including Asset Center, Risk Center, Alert Center, and Advanced Security Management. CSC supports periodic detection of six major risk categories: port risks, vulnerability risks, weak password risks, content risks, cloud resource configuration risks, and service exposure risks, enabling continuous monitoring of enterprise security status. It also centrally ingests log data from Cloud Firewall, Web Application Firewall, and Host Security, providing unified auditing, analysis, aggregation, visualization, and tracking of alert logs. For network monitoring and protection, customers can opt for Flow Logs (FL) to perform real-time, non-intrusive out-of-band collection, storage, and analysis of network traffic, addressing needs such as troubleshooting, architecture optimization, security detection, and compliance auditing. Tencent Cloud also offers EdgeOne (EO) platform, an edge security and acceleration platform that delivers security protection and acceleration services to customers based on Tencent's global edge nodes. Equipped with features

No.	Domain	Summary of Controls	Tencent Cloud's Response
			including DDoS protection, intelligent web protection, BOT/crawler attack protection, and DNS resolution, EdgeOne supports customers in configuring custom access control rules tailored to their business requirements. In addition, customers can use Anti-DDoS service to mitigate DDoS attack risks. Powered by abundant and high-quality DDoS protection resources and continuously evolving proprietary and AI-driven detection algorithms, this service effectively defends against DDoS attacks and ensures the stable and secure operation of customers' businesses. To assist customers in complying with regulatory requirements, Tencent Cloud has deployed an internal network monitoring system to monitor and trigger alerts for network devices such as routers, firewalls, and network servers. Multiple measures including permission control and approval workflows are implemented to strictly prohibit unauthorized access to internal network resources. Tencent Cloud has also deployed Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance auditing of command operations and login behaviors, and will trigger alerts upon detection of malicious programs or abnormal activities. Tencent Cloud follows up on and resolves identified security issues through its ticketing system. In terms of data center monitoring, Tencent Cloud requires data center operators to equip data centers with a 24/7 blind-spot-free video surveillance and alert

No.	Domain	Summary of Controls	Tencent Cloud's Response
			system, assign dedicated security personnel on duty at the security room, and ensure that surveillance records are securely retained for a sufficient period of time.
			Customers shall implement vulnerability scanning and penetration testing to identify and remediate security vulnerabilities and issues in the system.
			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 recommendations to help customers enhance system security and support verification after vulnerability remediation.
P14-2	Set up functions for protection against unauthorized access from external network	[Basic] Conduct Vulnerability Assessments and Penetration Testing	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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			to risk disposal.
			To assist customers in complying with regulatory requirements, Tencent Cloud has established an internal regular vulnerability scanning and penetration testing mechanism. Internal vulnerability scanning of Tencent Cloud typically covers web vulnerabilities, component vulnerabilities, configuration scanning, etc. It uses a vulnerability scanning system to automatically generate scanning tasks for vulnerability detection of assets in the cloud environment, followed by the analysis, classification and remediation of detected vulnerabilities. In terms of penetration testing, the Tencent Cloud Security Team conducts regular full-link large-scale penetration tests, and flexibly carries out targeted penetration tests before the launch of new products or in the event of major changes. Test results are notified to the relevant responsible departments through security work orders, which shall promptly perform vulnerability remediation or implement other compensating control measures to ensure that exploitable vulnerabilities identified in penetration tests are properly addressed. In addition, Tencent Cloud regularly conducts red-blue team exercises to simulate and defend against cyberattacks in real - world scenarios.
P15	Set up functions for protection against unauthorized access from external network	[Basic] Limit Devices Accessible from External Networks to the Minimum Necessary. In the case of cloud services, it is necessary to confirm with the cloud provider whether it is possible to restrict source IP addresses for management interfaces, depending on the access	Customers shall restrict externally accessible communication paths and communication-related equipment to the minimum necessary scope to prevent unauthorized access. Tencent Cloud APIs provide interfaces for various resources of Tencent Cloud products, enabling customers to quickly operate cloud products through TencentCloud API. To assist customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
		method (GUI, CLI, API). Financial institutions should, based on these findings, limit access to management interfaces to the minimum necessary for each access method.	with access protection, Tencent Cloud APIs support HTTPS transmission encryption, implement interface authentication via multiple SDK signature mechanisms (e.g., PHP, Python, Java, .Net, Node.js, etc.), prevent replay attacks by limiting the validity period of request signatures through timestamps, and support signature encryption. Tencent Cloud has integrated API monitoring and management functions, allowing customers to configure API interface status monitoring required by their businesses through the console. Meanwhile, Tencent Cloud provides API interface protection capabilities, which can effectively eliminate the risks of API invalidation or abuse. Customers can also 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. 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 network access control. Tencent Cloud also offers Cloud Firewall (CFW) to support customers in inbound and outbound access filtering. CFW access control rules support domain name filtering and traffic filtering based on geographic location requirements, enabling focused protection of core assets. In addition, EdgeOne (EO) platform, the edge security and acceleration platform, provides customers with security protection and acceleration services based on Tencent's global edge nodes. It is equipped with functions including DDoS protection, intelligent web protection, BOT/crawler attack protection, and DNS resolution, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			supports customers in configuring custom access control rules according to business needs. To assist customers in complying with regulatory requirements, Tencent Cloud has deployed mature network security architecture. It adopts multiple protection mechanisms such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, network logical isolation, and web application security to detect, filter and block malicious network traffic in a timely manner, thereby protecting Tencent Cloud's network security. Tencent Cloud regularly reviews the security policies and parameter settings of network devices such as routers, firewalls and network servers to ensure their effectiveness.
P16	Response Measures in the Event of Illegal Activities	[Basic] Implement Monitoring Functions for Unauthorized Access. In the case of cloud services, it is necessary to clarify the responsibility boundary between the cloud provider and the cloud user regarding monitoring of unauthorized access via the internet. Based on this, confirm the cloud provider's specific measures. Key points for confirmation include: (1) Devices and resources subject to unauthorized access monitoring (2) Notification to users upon detection of unauthorized access (3) Automatic suspension of IDs after repeated failed login attempts (4) Conditions and limitations when introducing third-party tools for unauthorized access	Customers shall monitor access failures and unauthorized access. When using cloud services, customers shall confirm with the cloud service provider the respective scope of responsibilities of the provider and the customer regarding unauthorized access monitoring, as well as the specific measures available from the cloud service provider. Through the Cloud Access Management (CAM) console, Tencent Cloud provides customers with secure permission assignment and sub-user management capabilities. CAM enables customers to define which actions and resources each user or role can access. Customers can also enable MFA for both primary and sub-accounts to enhance account security. CloudAudit provides comprehensive logging and continuous monitoring of user activities and API usage across Tencent Cloud infrastructure. Tencent Cloud also provides customers with Cloud Log Service (CLS), which

No.	Domain	Summary of Controls	Tencent Cloud's Response
		monitoring Financial institutions should implement internet-based unauthorized access monitoring based on these findings. If access control capabilities are insufficient, they should consider supplementing functionality through tools	supports configuring alert policies for one or more log topics. Alert policies periodically execute monitoring tasks, and send alert notifications when query and analysis results meet trigger conditions, facilitating customers' timely detection of abnormal issues. Customers can opt for Data Security Audit (CDS) to monitor abnormal operations targeting data. CDS is an AI-powered database security audit system that supports full-coverage audit and storage of all types of database session information, access operations and SQL statements within an enterprise network. It identifies malicious behaviors in operations based on multiple rule bases and threat detection engines, and promptly notifies administrators to take corresponding security protection measures. For security incidents that have occurred, CDS also supports auditing and analyzing years of logs, providing a reference basis for enterprises to reconstruct the full picture of security incidents and identify responsible parties. Tencent Cloud also provides customers with Cloud Log Service (CLS), which supports configuring alert policies for one or more log topics. Alert policies periodically execute monitoring tasks, and send alert notifications when query and analysis results meet trigger conditions, facilitating customers' timely detection of abnormal issues. Customers can opt for Cloud Data Security (CDS) to monitor abnormal operations targeting data. CDS is an AI-powered database security audit system that supports full-coverage audit and storage of all types of database session information, access operations and SQL statements within an enterprise network. It identifies

No.	Domain	Summary of Controls	Tencent Cloud's Response
			malicious behaviors in operations based on multiple rule bases and threat detection engines and promptly notifies administrators to take corresponding security protection measures. For security incidents that have occurred, CDS also supports auditing and analyzing years of logs, providing a reference basis for enterprises to reconstruct the full picture of security incidents and identify responsible parties. As a cloud service provider, Tencent Cloud is primarily responsible for the security of data center infrastructure and the cloud platform. Tencent Cloud makes available online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement on its international official website, which clearly define the content and service levels of the services provided by Tencent Cloud, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both the customer and Tencent Cloud, service terms and scenarios for agreement termination, dispute resolution mechanisms, notification mechanisms and other matters. Customers may also choose to sign offline agreements with Tencent Cloud to negotiate the terms and details of the agreement. In addition, considering that customers have different levels of control over different components when selecting different cloud service categories (e.g., IaaS, PaaS and SaaS services), Tencent Cloud has established a Cloud Security Shared Responsibility Model based on different cloud service categories. For details, please refer to Section 3 Tencent Cloud Security Responsibility Sharing Model.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud has formulated access control management specifications, defining access permission management requirements and relevant authorization mechanisms. Tencent Cloud requires all user accounts to use unique identifiers, and conducts admission authentication for employees through a zero-trust security management system. Tencent Cloud implements real-time security monitoring of the login status of employee accounts. Upon detection of any abnormal login behavior, the IT security system will immediately contact the account owner for verification and handling, and record relevant events in detail. For internal terminals, operating systems, applications and network devices, Tencent Cloud has configured policies for limiting the number of login failures and session timeouts, and has set login restriction policies for unauthorized access, so as to effectively monitor and alert on unauthorized access attempts.
P19	Response Measures in the Event of Illegal Activities	[Basic] Prepare Response and Recovery Measures for Unauthorized Access. In the case of cloud services, it is necessary to confirm the division of responsibilities between the cloud provider and the cloud user regarding measures to prevent the spread of unauthorized access and recovery procedures. Examples of measures provided by the cloud provider include: (1) The cloud provider's measures to prevent the spread of unauthorized access (2) The cloud provider's recovery	Customers shall define clear measures and recovery procedures to address unauthorized access. In the event of unauthorized access, customers shall analyze the root causes and then adopt countermeasures to prevent recurrence of similar incidents. When using cloud services, customers shall confirm with the cloud service provider the respective scope of responsibilities of the provider and the customer in preventing unauthorized access and implementing recovery, as well as the measures provided by the cloud service provider to prevent the escalation of unauthorized access and the relevant recovery countermeasures/services available to customers. To help customers detect and respond to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		solutions for unauthorized access incidents	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.
		Financial institutions should establish their response and recovery plans based on these findings. If the cloud provider's measures are insufficient, institutions should consider supplementing functionality through tools.	In terms of incident response and handling, Tencent Cloud has formulated internal information security incident management specifications, established an information security reporting, response and handling mechanism and related processes, and uses an internal security operation system to record security incidents. For detected and identified security incidents, Tencent Cloud will analyze and classify the incidents based on factors such as incident nature, data sensitivity level and impact scope, and promptly notify the relevant responsible personnel to follow up on the handling of the incidents. Tencent Cloud has established a periodic incident analysis mechanism, which conducts multi-dimensional analysis of incidents on a regular basis (including incident type, occurrence frequency, impact scope and severity), and adopts preventive measures based on incident review and root cause analysis to avoid recurrence of similar incidents. To ensure the continuous availability of customers' businesses, Tencent Cloud has formulated detailed disaster recovery plans for cloud products and critical processes, and conducts regular drills in strict accordance with requirements to ensure the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			timeliness and feasibility of these disaster recovery plans. Meanwhile, in terms of business continuity management and disaster recovery, Tencent Cloud has obtained the international standard certification of ISO/IEC 22301 Business Continuity Management System. Tencent Cloud has built a comprehensive business continuity management system, standardized processes related to business continuity management, covering business impact analysis, business continuity planning, emergency response and disaster recovery, emergency drills and testing, crisis management, etc. Tencent Cloud has also defined internal and external communication strategies during disaster incidents and established a contact list. Tencent Cloud reviews its disaster recovery plans annually based on the results of business impact analysis and updates them as needed.
P20	Prevention Countermeasures Against Malicious Programs	[Basic] Implement Defense Measures Against Malicious Programs such as Computer Viruses. In the case of cloud services, it is necessary to confirm with the cloud provider their defense measures against virus intrusion and program tampering by malicious programs. Financial institutions should implement defense measures based on these findings. If the cloud provider's functions are insufficient, supplement with additional tools.	Customers shall adopt preventive measures against malicious programs such as computer viruses. When using cloud services, customers shall confirm with the cloud service provider the countermeasures it implements to prevent intrusions by computer viruses and tampering by malicious programs, including protective functions offered by the provider such as WAF, IPS, firewalls, and antivirus software. Customers can leverage Cloud Workload Protection Platform (CWPP) to provide security protection for cloud hosts. Based on accumulated massive threat data, CWPP uses machine learning to deliver security protection services such as hacker intrusion detection and vulnerability risk alerts for customers, covering core security functions including brute force password cracking prevention, abnormal login notifications,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Trojan file detection, and high-risk vulnerability detection. These features address the major cybersecurity risks currently faced by servers. Tencent Cloud also provides customers with protective products such as Cloud Firewall and Web Application Firewall. Cloud Firewall (CFW) mainly provides protection for different network perimeters, supporting proactive firewall ACL control, real-time IPS interception, virtual patching, and malicious code detection. It can meet the DMZ zone requirements in traditional networks, realize focused protection of core assets, and enable fine-grained isolation and control between VPCs. Web Application Firewall (WAF) is capable of addressing security protection issues for websites and web services such as web attacks, intrusions, vulnerability exploitation, malicious code injection, content tampering, backdoor infiltration, and web crawling. To assist customers in complying with regulatory requirements, Tencent Cloud has established a network defense-in-depth system and deployed a mature network security architecture. It adopts multiple protection mechanisms including firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, network logical isolation, and web application security to timely detect, filter, and block malicious network traffic, thereby protecting Tencent Cloud's network security. In terms of physical host security, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools

No.	Domain	Summary of Controls	Tencent Cloud's Response
			adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance auditing of command operations and login behaviors, and will trigger alerts upon detection of malicious programs or abnormal activities. Tencent Cloud follows up on and handles alert events through its ticketing system.
P21	Prevention Countermeasures Against Malicious Programs	[Basic] Implement Detection Measures for Malicious Programs such as Computer Viruses. In the case of cloud services, financial institutions must confirm with the cloud provider the detection measures in place for malicious programs within the cloud service. Financial institutions should implement detection measures based on the above confirmation results, leveraging functions provided by cloud providers and security vendors.	Customers shall adopt appropriate detection countermeasures to identify the intrusion or implantation of malicious programs such as computer viruses. When using cloud services, customers shall confirm with the cloud service provider the countermeasures implemented in the cloud services for detecting malicious programs, and adopt corresponding detection countermeasures based on the confirmation results. Customers can leverage Cloud Workload Protection Platform (CWPP) to provide security protection for cloud hosts. Based on accumulated massive threat data, CWPP uses machine learning to deliver security protection services such as hacker intrusion detection and vulnerability risk alerts for customers. It includes core security functions such as brute force password cracking prevention, abnormal login notifications, Trojan file detection, and high-risk vulnerability detection, addressing the major cybersecurity risks currently faced by servers. Tencent Cloud also provides customers with Cloud Security Center (CSC), a one-stop security management platform. It can collect threat alerts and logs from Cloud Firewall and Web Application Firewall, and conduct automated analysis and investigation of the data using Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Cloud threat intelligence and proprietary security knowledge base, providing customers with centralized capabilities for threat detection, investigation and disposal. Meanwhile, multiple log products and services such as Tencent Cloud Cloud Log Service (CLS) support customers to download cloud - side logs to local devices for review, or forward them to designated third - party systems (including customers' local SIEM/SOC platforms) through functions such as log download, log export and log forwarding. In terms of physical host security, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance auditing of command operations and login behaviors, and will trigger alerts upon detection of malicious programs or abnormal activities. Tencent Cloud follows up on and handles alert events through its ticketing system.
P22	Prevention Countermeasures Against Malicious Programs	[Basic] Implement Measures in the Event of Damage from Malicious Programs such as Computer Viruses. In the case of cloud services, financial institutions must confirm with the cloud provider the available functions and tools that can be used by the institution when damage occurs due to viruses or other malicious programs, to assist in developing response	Customers shall formulate measures to address damages caused by malicious programs such as computer viruses. When using cloud services, customers shall confirm with the cloud service provider the available functions and means in the event of damages caused by malicious programs, including whether the automation of system shutdown and recovery can be achieved. Customers can use Cloud Workload Protection Platform (CWPP) to detect vulnerabilities in Linux software, Windows

No.	Domain	Summary of Controls	Tencent Cloud's Response
		procedures. Financial institutions should establish their response and recovery measures—from incident detection to full recovery—based on the above confirmation results.	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 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 assist customers in complying with regulatory requirements and promptly containing damages caused by malicious programs, Tencent Cloud supports the reporting of internal and external vulnerabilities and threat incidents by deploying internal vulnerability scanning platforms and external vulnerability collection platforms. Tencent Cloud will log detected security vulnerabilities into the ticketing system and assign relevant personnel to handle and remediate them within the specified time limit.

5.2.2 General System Operation and Maintenance

No.	Domain	Summary of Controls	Tencent Cloud's Response
P23	Compilation and Improvement of	[Basic] Establish Routine Operation Manuals.	Customers shall formulate and maintain manuals covering various daily operation

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Operation and Maintenance Manuals	In the case of cloud services, financial institutions must document the operations and procedures for using cloud services in manuals.	procedures (including operation steps). When using cloud services, customers shall document the operation and procedures of cloud services in the form of manuals. The operation procedures, user manuals and other documentation for Tencent Cloud products have been formalized and are available to customers via the official website. Tencent Cloud also provides customers with Tencent Cloud training and certification programs based on Tencent Cloud product knowledge and relevant professional capabilities, so as to enhance customers' technical proficiency and cloud service competency. In addition, Tencent Cloud offers customers multiple support channels, including 24/7 ticketing service, 24/7 hotline, intelligent customer service and self-service, to continuously address customer inquiries and feedback. Tencent Cloud's customer service team and technical experts will provide customers with prompt and effective support. Internally, Tencent Cloud has also formulated operation and maintenance (O&M) management specifications to provide operational guidelines and requirements for the daily O&M activities of O&M personnel. Tencent Cloud leverages a sophisticated tool-based and automated O&M management platform to administer O&M operations. It has also defined detailed O&M security red lines and conducts regular internal O&M security reviews.
P24	Compilation and Improvement of Operation and Maintenance Manuals	[Basic] Establish Manuals for System Failures and Disasters.	Customers shall formulate manuals for use in the event of failures or disasters, which shall include alternative measures, recovery procedures and response methods to be adopted when such incidents occur.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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, built a comprehensive business continuity management system, formulated business continuity management regulations, standardized processes related to business continuity management, and obtained the international standard certification of ISO/IEC 22301 Business Continuity Management System. Based on the results of business impact analysis of cloud products and services, Tencent Cloud has formulated differentiated response strategies, and developed detailed disaster recovery plans for cloud products and critical processes. These strategies and plans cover various aspects including venues, personnel, equipment, systems, information/data, and business priorities. Tencent Cloud conducts regular drills in strict accordance with requirements to ensure the feasibility of these plans.
P25	Access Right Management	[Basic] Clearly Define Access Rights to Resources and Systems. In cloud environments, financial institutions must confirm with the cloud provider the details and methods for setting access rights. Financial institutions should establish access rights based on job roles and responsibilities using the above confirmation results. If available permission types are insufficient, consider supplementing functionality through tool integration.	Customers shall define the owners of access permissions for computer systems and important documents, and restrict such permissions to the minimum necessary scope. When using cloud services, customers shall confirm with the cloud service provider the configuration details and methods of access permissions. <u>Cloud Access Management (CAM)</u> enables customers to securely and granularly manage access to Tencent Cloud products and resources. The root user account holds full access permissions to the resources under its name by default, and can create sub-users and assign identity IDs, credentials, and permissions to them. CAM also supports the use of <u>CloudAudit</u>

No.	Domain	Summary of Controls	Tencent Cloud's Response
			to conduct supervision, compliance checks, operation audits, and risk audits on Tencent Cloud account activities. Tencent Cloud also provides Bastion Host (BH), which supports fine-grained authorization based on dimensions such as users, assets, accounts, and operation permissions, ensuring that the permissions held by users are the minimum required for them to access assets and complete work tasks. Bastion Host also features operation audit functionality, which records and analyzes user operation logs to enable effective traceability of security incidents. To assist customers in complying with regulatory requirements, Tencent Cloud has clarified internal access permission management requirements and relevant authorization mechanisms, and permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights.. Tencent Cloud maintains records of the identity information of personnel corresponding to job roles and the permission levels of various business systems, and conducts regular internal permission reviews to prevent permission abuse and misuse. Meanwhile, Bastion Host has been fully deployed in Tencent Cloud's production environment to centrally control the administrator account permissions of backend system components of Tencent Cloud. Internal O&M personnel are required to obtain authorization approval to access the Bastion Host, and only specific internal O&M personnel of Tencent Cloud are granted access. Two-factor authentication is mandatory for logging into the Bastion Host. O&M operation records are centrally stored on a log

No.	Domain	Summary of Controls	Tencent Cloud's Response
			platform, and Tencent Cloud's internal audit team conducts regular reviews of these logs.
			Customers shall take measures to prevent the disclosure of information such as passwords, including reminding users to exercise caution and avoiding the use of weak passwords.
			<u>Cloud Access Management (CAM)</u> enables customers to securely and granularly manage access to Tencent Cloud products and resources. The root user account holds full access permissions to the resources under its name by default, and can create sub-users and assign identity IDs, credentials, and permissions to them. Users can modify sub-user password policies through the CAM console, including details such as password complexity, length, and validity period. To prevent password leakage, Tencent Cloud encrypts customer passwords using SHA256 hash algorithm with salt processing, and refrains from storing passwords in plaintext.
P26	Access Management	Right [Basic] Implement Measures to Prevent Password Disclosure.	To assist customers in complying with regulatory requirements, Tencent Cloud has formulated internal access control management specifications, which mandate that all user accounts adopt unique identifiers. It also sets password policies for employee accounts based on security baselines, covering password length, complexity, lockout, and reset mechanisms. Tencent Cloud conducts admission authentication for employees through a zero-trust security management system, and users are required to complete two-factor authentication before accessing internal resources.
P27	Access	Right [Basic] Clearly Define Procedures	Customers shall define access authorization

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Management	for Granting and Reviewing Access Rights. In cloud environments, financial institutions must confirm with the cloud provider the procedures and functionalities related to granting and reviewing access rights to cloud resources. Based on the above confirmation, financial institutions should establish internal procedures for granting and reviewing access rights. If the cloud provider's native capabilities are insufficient, consider integrating third-party tools to enhance functionality.	procedures as well as access authorization review procedures for various types of resources and systems. When using cloud services, customers shall confirm with the cloud service provider the functions related to resource permission granting available in its cloud services, and formulate internal permission granting and review procedures based on the confirmation results. Customers can use Cloud Access Management (CAM) to assign resource permissions to sub-users through methods such as tagging, achieving granular access control over cloud resources. Tencent Cloud also provides customers with Bastion Host (BH), which supports fine-grained authorization based on dimensions including users, assets, accounts, and operation permissions, ensuring that the permissions held by users are the minimum required for them to access assets and complete work tasks. In addition, user guides, operation procedures and other documentation for cloud products such as CAM and BH have been formalized and made available to customers via the official website, which customers can refer to for permission allocation and management. Internally, Tencent Cloud has also formulated access control authorization policies and permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights. Tencent Cloud maintains records of the identity information of personnel corresponding to job roles and the permission levels of various business systems, and conducts regular internal permission reviews to prevent permission abuse and misuse.

No.	Domain	Summary of Controls	Tencent Cloud's Response
P30	Access Right Management		Customers shall formulate procedures for the generation, distribution, use, and custody of encryption keys, and specify response measures in the event of key leakage. When using cloud services, customers shall confirm with the cloud service provider the details of the key management services it offers, and formulate internal procedures related to the full lifecycle of keys based on the confirmation results.
		[Basic] Clearly Define Cryptographic Key Operation and Management Procedures.	To help customers safeguard the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS). KMS enables customers to easily create and manage keys, meets their key management needs across multiple applications and businesses, and complies with regulatory and compliance requirements. KMS seamlessly integrates with the encryption features of services such as Object Storage, Distributed Database, and Cloud Block Storage, facilitating easy adoption by customers.
		In cloud environments, financial institutions must confirm the details of the cryptographic key management services provided by the cloud provider to establish comprehensive lifecycle procedures (generation, distribution, storage, revocation, renewal, disposal, retention, etc.).	KMS generates and protects keys based on FIPS-140-2 certified Hardware Security Modules (HSMs). It adopts secure data transmission protocols, deploys multi-data-center distributed clustered services with hot backup, and implements cold backup deployment of underlying HSM devices across dual data centers, ensuring the high availability of the key management system. To ensure the security of ciphertext and reduce the risk of key compromise or abuse, KMS supports regular key rotation. After rotation, KMS remains compatible with ciphertext encrypted using the previous key, without causing any impact on customers' businesses. KMS adopts secure and reliable methods to delete invalid,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			revoked, or leaked keys. Deleted keys cannot be recovered, and the encrypted data associated with such keys will no longer be decryptable. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated internal encryption and key management standards, specifying security requirements for the entire process of key application, generation, storage, use, transmission, update, and destruction. All operations related to the key lifecycle shall comply with the basic requirements of dual control, rigorous handover, proper custody, and timely update. During the use of keys, it is also required to follow the principles of segregation of duties, strict approval, and identity-verified operations. In addition, operation logs for business keys shall be retained and subject to regular operational audits. Furthermore, Tencent Cloud manages the full lifecycle of keys by comprehensively considering factors such as key purpose, sensitivity of the data protected by the keys, and the likelihood and impact of key leakage.
P31	Operational Proficiency Training	[Basic] Conduct Education and Training for Operational Proficiency. In cloud environments, financial institutions should be aware that system changes due to cloud services may occur frequently when planning training: (1) Manual revisions may be driven not only by internal factors (e.g., changes to business applications) but also by external factors such as changes to cloud provider features. Training should be conducted as needed based on	Customers shall conduct operation-related education and training. When using cloud services, customers shall take into account changes in cloud service functions as well as system changes that may result from such cloud service changes, revise relevant manuals in a timely manner, and conduct education and training when necessary based on the revised content. The operation procedures, user manuals and other documentation for Tencent Cloud products have been formalized and are available to customers via the official website. Tencent Cloud also provides customers with Tencent Cloud training and certification programs based on

No.	Domain	Summary of Controls	Tencent Cloud's Response
		manual updates. (2) In addition to manuals and references provided by the cloud provider, information published on the provider's website should be referenced, and training conducted as necessary.	Tencent Cloud product knowledge and relevant professional capabilities, so as to enhance customers' technical proficiency and cloud service competency. For changes to products, infrastructure, and network configurations that may affect the external environment, Tencent Cloud will notify customers via announcements, emails, cloud console, and/or other appropriate channels. Internally, Tencent Cloud has also established a sound training mechanism, requiring regular employees, consultants, interns, and outsourced staff to complete training courses. Tencent Cloud provides a diverse range of training programs, including mandatory training for all employees, specialized training for key positions, and optional professional courses. The content covers areas such as basic security awareness, office security, vulnerability identification and defense, privacy protection, emergency response, R&D security specifications, and data security requirements.
P32	Countermeasures Against Computer Viruses	[Basic] Implement Computer Virus Countermeasures.	Customers shall define clear processes for the prevention, detection, and recovery of computer viruses to guard against the intrusion and infection of computer viruses and similar threats. Customers can leverage Cloud Workload Protection Platform (CWPP) to provide security protection for cloud hosts. Based on accumulated massive threat data, CWPP uses machine learning to deliver security protection services such as hacker intrusion detection and vulnerability risk alerts for customers. It includes core security functions such as brute force password cracking prevention, abnormal login notifications, Trojan file detection, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			high-risk vulnerability detection, addressing the major cybersecurity risks currently faced by servers. To assist customers in complying with regulatory requirements, in terms of server antivirus protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions including antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance auditing of command operations and login behaviors, and will trigger alerts upon detection of malicious programs or abnormal activities. For the usage management of office terminals, Tencent Cloud has formulated internal software security specifications, which clarify the software usage restrictions on office terminals (including laptops and workstations). It leverages application whitelisting technology to only allow the operation of known and trusted programs, thereby reducing the risk of malware intrusion. Tencent Cloud also implements terminal management and control through a zero-trust security management system, and achieves all-round security protection including ransomware prevention, phishing attack prevention, and internal lateral movement prevention by virtue of security capabilities such as virus scanning and removal, vulnerability remediation, and proactive defense.
P33	External Connection Management	[Basic] Clearly Define Connection Agreement Contents.	Customers shall specify details including connection methods, data formats, and data content in contracts signed for data

No.	Domain	Summary of Controls	Tencent Cloud's Response
			transmission and reception via line connections. Tencent Cloud provides API interfaces for customers' external data transmission, which clearly define the transmission protocols, transmission formats, and transmission content. In addition, the cloud API interfaces offered by Tencent Cloud's products are equipped with security capabilities such as HTTPS encryption, signature verification, and status monitoring, providing port-level communication security guarantees for customers' businesses.
P34	External Connection Management	[Basic] Clearly Define Operational Management Methods for External Connections. In cloud environments, financial institutions must confirm that cloud service providers meet the institution's security standards. Key verification points include: Whether vulnerabilities—especially in components involving Internet connectivity—are properly addressed within the cloud provider's operational management scope. Examples of areas managed by the cloud provider: (1) Software version updates for network equipment used within the cloud (2) Software version updates for virtualization platforms and managed services used in the cloud.	Customers shall define operation and maintenance (O&M) management methods for external connections. When using cloud services, customers shall confirm with the cloud service provider whether vulnerabilities are properly addressed within its O&M scope, and whether version upgrades for network devices and virtualization platform-related software are properly managed. In terms of remote O&M security, Tencent Cloud provides customers with VPN Connection. VPN Connection encrypts transmitted data using the Internet Key Exchange (IKE) protocol and IPsec, establishing a secure and trusted data tunnel over the Internet to ensure data security during transmission. The VPN gateway features high reliability, adopting an active-active standby architecture at the underlying layer to ensure uninterrupted communication sessions with zero awareness to upper-layer applications. Tencent Cloud has also established internal procedures governing remote access for employees. Employees may only use trusted devices registered on Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			to remotely access Tencent Cloud's office network and daily office systems through encrypted communication channels. Tencent Cloud maintains remote access logs to record user operation behaviors. Meanwhile, 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 storing customer data via a bastion host. Backend O&M operation records are centrally stored on a log platform, and Tencent Cloud's internal audit team conducts regular reviews of the recorded information. For vulnerability and patch management, Tencent Cloud identifies the latest patches and conducts thorough security testing on patches prior to installation to ensure their safety. Tencent Cloud regularly notifies internal business teams to perform patch upgrades and installations, and uses endpoint detection tools to periodically scan patch installation status. Automated alert tickets are generated for devices with overdue patch installations. In addition, Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform for reporting internal and external vulnerabilities and threats. Security vulnerability tickets are logged in the security operation system and assigned to relevant responsible personnel for resolution within a specified timeframe. Furthermore, Tencent Cloud's security research team integrates vulnerability protection capabilities into Tencent Cloud's

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Web Application Firewall system in the form of virtual patches to ensure the overall security of the cloud computing platform. In terms of network device management, Tencent Cloud has formulated a set of network security configuration standards and security baseline standards to standardize the security configuration management of network devices and similar assets. Tencent Cloud's security team conducts regular reviews of the security policies and parameter settings of network devices such as routers, firewalls, and network servers to ensure their effectiveness. Additionally, Tencent Cloud has deployed an internal network monitoring system to monitor and trigger alerts for network devices including routers, firewalls, and network servers.

5.2.3 Operational Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
P35	Operational Control	[Basic] Verify Operator Qualifications. In the case of cloud services, it is necessary to confirm whether the cloud service provider has implemented stronger qualification verification mechanisms, considering that financial institutions' operators may access systems via the Internet (not necessarily from a fixed, secure location).	Customers shall verify the qualifications of operators to prevent unauthorized use of computer systems. When using cloud services, customers shall confirm with the cloud service provider whether it can provide robust qualification verification methods. <u>Cloud Access Management (CAM)</u> enables customers to securely and granularly manage access to Tencent Cloud products and resources. The root user account holds full access permissions to the resources under its name by default, and can create sub-users and assign identity IDs, credentials, and permissions to them. CAM supports multi-factor authentication through various methods, including verification via MFA devices or mobile verification codes, so as to verify the security and reliability of the user identity

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and environment prior to login and sensitive operations. Tencent Cloud also provides Bastion Host (BH), which supports fine-grained authorization based on dimensions such as users, assets, accounts, and operation permissions, ensuring that the permissions granted to users are the minimum required for them to access assets and complete work tasks. Bastion Host also features operation audit functionality, which records and analyzes user operation logs to enable effective traceability of security incidents. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated internal access control authorization policies and a segregation of duties matrix mechanism. It mandates the use of unique identifiers for all user accounts and sets password policies for employee accounts based on security baselines. Tencent Cloud conducts admission authentication for employees through a zero-trust security management system; users are required to log in to their accounts and complete two-factor authentication via the system before accessing internal resources. Meanwhile, Bastion Host has been fully deployed in Tencent Cloud's production environment to centrally control the administrator account permissions of backend system components. Internal O&M personnel must obtain authorization approval to access the Bastion Host, and only specific internal O&M personnel of Tencent Cloud are granted such access. Two-factor authentication is mandatory for logging into the Bastion Host.
P36	Operational Control	[Basic] Clearly Define Operation Request and Approval Procedures.	Customers shall define procedures for operation requests and approvals to prevent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			unauthorized use of computer systems. Through the Cloud Access Management (CAM) console, Tencent Cloud provides customers with secure permission assignment and sub-user management capabilities. CAM enables customers to define which actions and resources each user or role can access. Customers can also enable MFA for both primary and sub-accounts to enhance account security. CloudAudit provides comprehensive logging and continuous monitoring of user activities and API usage across Tencent Cloud infrastructure. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated internal access control management specifications and corresponding authorization policies, clarifying the approval procedures required for accessing and operating host operating systems, application systems, network devices, and other assets, so as to prevent unauthorized access by personnel.
P37	Operational Control	[Basic] Clearly Define the Operation Execution Framework. For cloud services, it is necessary to confirm that the cloud provider has implemented measures to prevent operator errors and unauthorized use. Examples of verification points include: (1) Scope and content of operation logs (2) Function to record or video capture operator screens	Customers shall define relevant mechanisms for operation execution, including the composition of operator teams and operation procedures. When using cloud services, customers shall take measures to prevent misoperations and unauthorized use. To help customers prevent misoperations and unauthorized operations, Tencent Cloud provides CloudAudit. CloudAudit enables customers to supervise Tencent Cloud account activities, conduct compliance checks, operation audits and risk audits, and supports online viewing of operation records of the Tencent Cloud Console and cloud APIs within the most recent 90 days. Bastion Host (BH) is also capable of recording and auditing users'

No.	Domain	Summary of Controls	Tencent Cloud's Response
			O&M operations, and supports real restoration of user operation behaviors through playback, ensuring effective traceability of security incidents. In addition, the operation procedures, user manuals and other documentation for Tencent Cloud products have been formalized and are available to customers via the official website. Tencent Cloud also provides customers with Tencent Cloud training and certification programs based on Tencent Cloud product knowledge and relevant professional capabilities, so as to enhance customers' technical proficiency and cloud service competency. Internally, Tencent Cloud has also formulated O&M management specifications to provide operational guidelines and requirements for O&M personnel's daily O&M activities. Tencent Cloud leverages a sophisticated tool-based and automated O&M management platform to administer O&M operations and strictly controls change time windows through internal O&M management mechanisms to ensure that all O&M requests can be completed within the specified time. Tencent Cloud has also defined detailed O&M security red lines and conducts regular internal O&M security reviews. To ensure that operations in the production environment are controllable and traceable, all backend O&M operation records are meticulously documented, centrally stored on a log platform, and the internal audit team of Tencent Cloud regularly conducts troubleshooting and traceability of suspicious operations during the O&M process.
P38	Operational Control	[Basic] Record and Verify Operations.	Customers shall record and verify operations to validate the legitimacy of such operations.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			<u>CloudAudit</u> supports supervision, compliance checks, operation audits, and risk audits of Tencent Cloud accounts. Customers can leverage CloudAudit to log, continuously monitor, and retain account activities related to operations across the entire Tencent Cloud infrastructure. Customers may also opt for <u>Data Security Audit (CDS)</u> to monitor abnormal operations targeting data. CDS is an AI-powered database security audit system that supports full-coverage audit and storage of all types of database session information, access operations, and SQL statements within an enterprise network. Based on multiple rule bases and threat detection engines, it identifies malicious behaviors in operations and promptly notifies administrators to take corresponding security protection measures. For security incidents that have occurred, CDS also supports auditing and analyzing years of logs, providing a reference basis for enterprises to reconstruct the full picture of security incidents and identify responsible parties. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated O&M management specifications to provide operational guidelines and requirements for O&M personnel's daily O&M activities. Tencent Cloud has also defined detailed O&M security red lines and conducts regular internal O&M security reviews. In addition, Bastion Host has been fully deployed in Tencent Cloud's production environment, and all O&M operations in the production environment must be performed through the Bastion Host. To ensure that operations in the production environment are controllable and traceable, all backend O&M operation records are meticulously

No.	Domain	Summary of Controls	Tencent Cloud's Response
P39	Data Management	[Basic] Ensure Backup of Data Files. In cloud environments, if the cloud provider's backups can be used for business continuity and disaster recovery, the financial institution may not need to perform its own backups. However, it is necessary to verify the cloud provider's backup practices. Financial institutions must perform their own backups—including not only data files but also cloud environment configuration data—for any areas not covered by the cloud provider.	documented and centrally stored on a log platform. Tencent Cloud's internal audit team regularly conducts troubleshooting and traceability of suspicious operations during the O&M process.
			Customers shall back up important data files and define relevant management methods.
			Tencent Cloud data centers span across mainland China, the Asia-Pacific region, North America, and Europe, and are structured by regions and availability zones (AZs). Tencent Cloud regions are fully isolated from each other, and each region is further divided into multiple mutually isolated availability zones. Based on business development needs and data security requirements, customers can independently and flexibly deploy or back up data and systems across different regions or availability zones to meet business disaster recovery requirements. In addition, Tencent Cloud mandates that cloud products adopt a multi-data-center redundancy mechanism within a single region to ensure the business continuity of cloud services. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			through this mechanism to facilitate data recovery in disaster scenarios. Internally, Tencent Cloud has also formulated backup management procedures, and backs up collected and processed important data in accordance with relevant legal and regulatory requirements. For internal critical information, Tencent Cloud formulates differentiated backup policies based on data classification levels and conducts regular recovery testing. In compliance with backup policies, Tencent Cloud performs backups of servers, network devices, configuration files of application systems, logs, and other information to ensure timely recovery in the event of file corruption.
P40	Program Management	File [Basic] Clearly Define Program File Management Methods.	Customers shall define methods and procedures for managing program files (including source programs and load modules of software package programs, self-developed programs, and the like) to prevent tampering, damage, and other such incidents to the programs. To assist customers in managing program files, Tencent Cloud provides Cloud-Native Build (CNB) as part of its developer tools suite. CNB offers a complete developer toolchain and effectively enables full lifecycle support and management for R&D from requirement analysis to deployment. Its artifact repository can be used to store, manage and distribute artifacts generated during the software build process. Internally, Tencent Cloud has also established a set of information system secure development standards, and strived to integrate the ISO/IEC 20000 IT service management standard, ISO/IEC 27001 information security management system, and ISO/IEC 9001 quality management

No.	Domain	Summary of Controls	Tencent Cloud's Response
			system standard into the entire lifecycle of product secure development. It focuses on various stages including requirements, design, R&D, testing, delivery, and O&M to ensure that cloud products receive robust security control throughout their lifecycle. DevSecOps management mechanisms are embedded in Tencent Cloud's software development process to enable the rapid and continuous development, release and deployment of cloud products while upholding security standards. Tencent Cloud uses code repositories to manage the source code of self-developed projects, and has established corresponding authorized access management mechanisms that adhere to the principle of least privilege, assigning only the necessary access permissions to different roles based on their actual job scenarios. Tencent Cloud prohibits the unauthorized copying, transmission and distribution of source code to external parties.
P41	Program File Management	[Basic] Clearly Define Program File Management Methods.	Customers shall back up program files and define relevant protection and management methods for them. Various Tencent Cloud products and services including computing services, network services, storage services, database services, container and middleware services, and security services all feature high availability and have corresponding disaster recovery plans in place. For example, Cloud Object Storage (COS) supports redundant data storage across multiple architectures and devices, provides remote disaster recovery and resource isolation capabilities for user data, and achieves high data durability. Cloud Block Storage (CBS) backs up data by capturing point-in-time snapshots of CBS volumes, preventing data loss caused by

No.	Domain	Summary of Controls	Tencent Cloud's Response
			tampering and accidental deletion, and enabling rapid rollback in the event of service failures. In addition, Tencent Cloud builds or leases data centers in multiple locations worldwide in compliance with relevant international standards and local security requirements. At present, there are two data centers with independent power supply and network connections in Japan, which can support customers to store, process and back up data within Japan. Based on their business development needs and data security requirements, customers can independently and flexibly deploy and back up their data and systems across different regions or availability zones to meet their business disaster recovery requirements.
P42	Network Configuration Information Management	[Basic] Manage Network Configuration Information. In cloud environments, Financial institutions are necessary to confirm with the cloud service provider the security measures for the management interfaces used to access network devices.	Customers shall properly manage the configuration information of network devices to prevent unauthorized modifications to such information. Customers can 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 compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. In addition, Cloud Access Management (CAM), through its granular permission control capabilities, grants specific permissions to different personnel for different resources. Customers can also use CloudAudit to conduct supervision, compliance checks, operation audits, and risk audits on Tencent Cloud account

No.	Domain	Summary of Controls	Tencent Cloud's Response
			activities. CloudAudit supports online viewing of operation records of the Tencent Cloud Console and cloud APIs within the most recent 90 days. To assist customers in complying with regulatory requirements, Tencent Cloud has established a set of network security configuration standards and security baseline standards to implement standardized management of the security configurations of network devices and similar assets. Any changes to Tencent Cloud's network configuration information must go through the corresponding change and approval procedures. Meanwhile, Bastion Host has been fully deployed in Tencent Cloud's production environment, which is used to centrally control the relevant account permissions of network devices, and strictly prohibits unauthorized personnel from accessing internal network resources. Internal O&M personnel are required to obtain approval and authorization to access the Bastion Host, and those with authorized access must complete two-factor authentication to log in. All backend O&M operation records are centrally stored on a log platform, and Tencent Cloud's internal audit team conducts regular reviews of these records. In addition, for the physical access management of network devices, Tencent Cloud requires data center operators to establish a complete personnel access control security matrix in the access control authorization system based on personnel categories and access permissions, so as to effectively control the access and operation behaviors of all types of personnel. Tencent Cloud mandates that operators verify the identities of all visitors and staff entering and exiting the data centers and computer

No.	Domain	Summary of Controls	Tencent Cloud's Response
P43	Network Configuration Information Management	[Basic] Ensure Backup of Network Configuration Information.	rooms, inspect their personal belongings, and register the items they carry. Tencent Cloud also requires operators to equip data centers with a 24/7 blind-spot-free video surveillance and alarm system, which is monitored by the security room; surveillance records are stored securely and retained for a sufficient period of time.
			Customers shall be able to back up the configuration information of network devices and define relevant management methods for such backups.
			To ensure high availability of customers' networks, Tencent Cloud Virtual Private Cloud (VPC) adopts mature network virtualization technologies. It guarantees network high availability through a variety of technical measures including link redundancy, active-standby gateways, and cross-availability zone deployment of virtual private clouds, providing all-round protection for network security and stability at the link, network and data center levels. Meanwhile, Tencent Cloud Cloud Load Balancer (CLB) is deployed in a clustered architecture and automatically removes faulty instances in a timely manner to achieve high availability.
P44	Document Management	[Basic] Clearly Define Storage and Management Methods for	To assist customers in complying with regulatory requirements, Tencent Cloud has formulated backup management procedures and backs up collected and processed important data in accordance with relevant legal and regulatory provisions. Tencent Cloud backs up information such as configuration files and logs of servers, network devices and application systems in accordance with pre-defined backup policies, ensuring timely recovery in the event of file corruption.
			Customers shall define methods for managing O&M documents, including

No.	Domain	Summary of Controls	Tencent Cloud's Response
	During O&M	Operational Documents.	operating procedures, operation instructions, system-related materials, and terminal operation manuals required for data center operations and maintenance. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated relevant specifications and procedures for document management, standardizing document identification requirements such as document numbers, version numbers, distribution numbers, and release and implementation dates, so as to ensure that valid versions of applicable documents are available for use. Tencent Cloud primarily publishes and manages institutional documents through its internal institutional management platform. Such documents may only be published or revised on the platform upon multi-party review and approval, and are maintained by the corresponding document administrators. Document administrators are entitled to the permission to revise and update institutional documents, while users only have the right to view such documents on the platform. Tencent Cloud's internal file management platform enables employees to independently upload various work files and set custom read and write permissions for the files on their own.
P45	Document Management During O&M	[Basic] Ensure Backup of Documents Required for Disaster Recovery.	Customers shall back up documents required for recovery and define the corresponding management methods for such backups. To ensure that customers can respond rapidly and restore critical functions in the event of a cyber security incident, a variety of storage and database services provided by Tencent Cloud are equipped with backup capabilities and support requirements such as multi-redundancy backup and remote

No.	Domain	Summary of Controls	Tencent Cloud's Response
			disaster recovery. To assist customers in achieving timely disaster recovery, Tencent Cloud has designed and implemented a business continuity management framework adapted to its own cloud computing environment, built a comprehensive business continuity management system, and obtained the international standard certification for the ISO/IEC 22301 Business Continuity Management System. In terms of data backup, Tencent Cloud has formulated backup management procedures and backs up important collected and processed data in accordance with relevant legal and regulatory requirements. For internal critical information, Tencent Cloud formulates differentiated backup policies based on data classification levels and conducts regular recovery tests. For cloud-based customer data, Tencent Cloud provides customers with multiple storage replicas and backup services according to the functions of the relevant cloud products or services, and assumes liability for the provided data backup services in accordance with the provisions stipulated in the product service level agreements. For more information related to backup, please refer to the content in Clause 39 Data File Management of Section 5.2.3 in this Guide.
P46	Operation Monitoring	[Basic] Establish a System Monitoring Framework. In cloud environments, Financial institutions are necessary to confirm with the cloud service provider the monitoring targets, content, and methods, including the monitoring services and optional features they offer. Financial institutions should	Customers shall establish a monitoring system for system operation status, defining clear monitoring objects, monitoring content and monitoring methods. When using cloud services, customers shall confirm with the cloud service provider the monitoring services and optional functions it offers, and establish a monitoring system based on the confirmation results. To enable the monitoring and management

No.	Domain	Summary of Controls	Tencent Cloud's Response
		establish their monitoring framework based on these confirmations.	of system operation status, customers can use Tencent Cloud Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis and alerting for cloud products and resources. It collects various monitoring metrics automatically reported by cloud products such as CVMs and cloud databases, as well as custom-configured monitoring metrics reported by customers, and displays them through visual charts. It helps customers keep real-time track of cloud product resource utilization, application performance and cloud product operation status, and supports setting up alerts for metrics. In accordance with the configured alert rules, it notifies customers of business anomalies in a timely manner through methods such as message push. For the monitoring and management of infrastructure, Tencent Cloud has deployed an internal network monitoring system to monitor and issue alerts for network devices including routers, firewalls and network servers, and has also implemented Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance auditing of command operations and login behaviors, and trigger alerts upon detection of malicious programs or abnormal activities. Tencent Cloud follows up on and resolves identified security issues through its ticket system.

5.2.4 Management of Various Types of Equipment

No.	Domain	Summary of Controls	Tencent Cloud's Response
P47	Resource Management	[Basic] Monitor Resource Capacity and Usage. In cloud environments, confirm with the cloud provider how resource capacity and usage are monitored. In cloud environments, confirm with the cloud provider the following regarding managed resources: (1) Thresholds set for monitoring resource usage (2) Scaling policies that financial institutions can define (e.g., rules for auto-scaling based on demand)	Customers shall take appropriate measures to monitor the capacity and usage of various resources to prevent malfunctions or processing capacity degradation of computer systems. <u>Tencent Cloud Observability Platform (TCOP)</u> provides real-time monitoring, analysis and alerting services for cloud products and resources. It collects and displays, via visual charts, all monitoring metrics automatically reported by cloud products such as Cloud Virtual Machines (CVMs) and cloud databases, as well as custom-configured monitoring metrics submitted by customers, helping customers keep real-time track of cloud product resource utilization, application performance and cloud product operation status. TCOP supports setting up alerts for metrics and will promptly notify customers of business anomalies through methods such as message push in accordance with the configured alert rules. To facilitate customers' convenient capacity planning and adjustment, Tencent Cloud offers <u>Auto Scaling (AS)</u> service. AS can automatically detect the health status of instances and dynamically adjust the computing resources of CVMs based on customers' business needs, policies, and preconfigured scaling-out and scaling-in conditions, ensuring that an adequate number of CVM instances are always available to handle customers' application loads. Internally, Tencent Cloud has formulated a capacity management procedure, which includes forecasting capacity requirements based on business operation needs and developing an annual capacity management plan. Meanwhile, Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
P48	Equipment Management		Cloud uses an internal capacity monitoring platform to conduct real-time monitoring of capacity usage and identify capacity usage trends.
			Customers shall implement configuration and version management for the hardware and software constituting the systems to ensure the smooth execution of system introduction, change, decommissioning and fault response.
		[Basic] Manage Hardware and Software. In cloud environments, it is necessary to confirm with the cloud provider the configuration management features they offer. Financial institutions should perform configuration management based on these confirmations.	Customers can 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 compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources.
		In cloud environments, it is necessary to confirm with the cloud provider how changes to base software (OS, middleware, etc.) will be communicated to the financial institution. Financial institutions should perform configuration based on these confirmations	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. In terms of configuration management, Tencent Cloud has established an internal set of network security configuration standards and security baseline standards, which are designed to standardize the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management of security configurations for network devices, firewalls, host server operating systems, databases and application systems. Tencent Cloud uses configuration scanning tools to continuously detect deviations between the configurations of operating systems, database management systems and virtual images and the established standards. For identified deviations, Tencent Cloud automatically generates security tickets and dispatches them to the responsible teams for timely rectification. In terms of change management, Tencent Cloud has formulated an internal set of management standards for product and configuration changes, defining all steps in the change process and the corresponding responsible persons to ensure that all changes undergo proper review, approval and testing prior to implementation. Tencent Cloud's change and release management procedures cover changes to configuration files, operating systems and databases. Prior to going live, all such changes must undergo business impact analysis and independent functional testing; a backup and rollback plan for the changes must be formulated and approved by the relevant responsible persons. Tencent Cloud's change and release system mandates that change operations can only be performed by authorized personnel, retains logs related to all changes and conducts regular audits of the logs. After a change is released, Tencent Cloud monitors the implementation of the change in the production environment and verifies the change results. In addition, for O&M change operations that may have an impact on customers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud operations team will promptly issue change notifications to the affected customers through official website, in-site messages and other channels. For the use of third-party and open-source products, Tencent Cloud has formulated supply chain security management requirements, specifying that security admission reviews must be conducted when introducing external components, and security hardening and defense measures must be implemented prior to going live to ensure that products pass the pre-launch security inspection. After a product is launched, continuous security O&M and inspections are carried out to resolve security issues in a timely manner. Tencent Cloud also conducts evaluations of the product's security operation status to identify security risks, urge suppliers to make improvements, and review the subsequent cooperation strategies with such suppliers.
P49	Equipment Management	[Basic] Clearly Define Equipment Management Methods.	Customers shall manage all types of equipment in computer systems, such as specifying responsible persons for management, maintaining equipment information, and controlling the entry and exit of equipment. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. To assist customers in meeting regulatory requirements, in terms of information asset management, Tencent Cloud has established information asset management standards and full-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. For equipment maintenance and entry-exit management, Tencent Cloud requires data center operators to formulate stringent access control policies for infrastructure and the physical environment in accordance with regional security requirements of different levels. All visitors and staff must undergo identity verification and personal belongings inspection when entering or exiting the data center, and the items they

No.	Domain	Summary of Controls	Tencent Cloud's Response
			carry shall be registered. Meanwhile, Tencent Cloud has established approval and inspection procedures for the entry and exit of equipment from computer rooms (e.g., for installation, operation, decommissioning or transfer-out). When equipment assets are warehoused or ex-warehoused, the on-site asset administrators in charge shall conduct stringent inspection and verification in accordance with the warehousing and ex-warehousing work orders. The handover of equipment assets for warehousing and ex-warehousing shall be carried out in a monitored handover area with camera coverage. Paper handover documents shall be retained for all entry-exit and handover procedures, and such documents shall be kept for three years.
P50	Equipment Management	[Additional] Implement Protective Measures for Network Equipment	Customers shall take appropriate protective measures for the network devices (such as MDF, IDF, routers, firewalls, etc.) used by systems processing important data. To assist customers in complying with regulatory requirements, Tencent Cloud has established network security management specifications and a network defense-in-depth system. Tencent Cloud has defined network security control and protection standards, as well as the corresponding roles and responsibilities, through management systems and procedures to ensure the secure operation of businesses hosted on Tencent Cloud's network. Meanwhile, Tencent Cloud has deployed an internal network monitoring system to monitor and issue alerts for network devices including routers, firewalls and network servers, and has implemented multiple measures such as permission control and approval

No.	Domain	Summary of Controls			Tencent Cloud's Response
					procedures to strictly prohibit unauthorized personnel from accessing internal network resources.
P51	Equipment Management	[Basic] Equipment Methods.	Clearly Equipment Maintenance	Define Maintenance	Customers shall conduct maintenance inspections on the equipment constituting computer systems and keep records of the inspection contents and results. To prevent hardware malfunctions, customers shall also perform preventive maintenance on a regular or ad hoc basis in accordance with the characteristics and importance of the equipment. To assist customers in complying with 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. Tencent Cloud conducts regular maintenance and upkeep of infrastructure and retains records of such activities. Personnel entering computer rooms to repair or maintain equipment must comply with the corresponding approval procedures and strictly implement all relevant rules of the computer rooms. Tencent Cloud has also deployed an internal network monitoring system to monitor and issue alerts for network devices such as routers, firewalls and network servers, and implemented Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. In addition, Tencent Cloud requires data center operators to arrange on-site staff to
P52	Equipment Management	[Additional] Preventive Equipment.	Implement Maintenance for		

No.	Domain	Summary of Controls	Tencent Cloud's Response
			conduct regular patrol inspections of critical equipment in server rooms, record inspection results, report abnormalities and resolve identified issues in accordance with pre-defined procedures. This ensures that potential safety hazards are detected and rectified in a timely manner, and the stable operation of equipment is maintained. Tencent Cloud also mandates that operators deploy monitoring systems to conduct 24/7 uninterrupted monitoring of pre-set metrics for critical data center equipment. An automatic alert will be sent to on-site staff immediately upon the occurrence of any abnormalities.
P53	Maintenance and Management of Computer-related Equipment	[Basic] Clearly Define Management Methods for Computer-Related Facilities (such as power supply, air conditioning, water supply/drainage, fire protection, security, monitoring, and communication lines)	Customers shall designate the persons responsible for managing the facilities associated with the operation of computer systems—including power supply, air conditioning, water supply and drainage, disaster prevention, security, monitoring and wiring systems—and define the corresponding management methods. They shall conduct management in accordance with the established methods and specify the response measures for equipment failures or disasters. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated physical security management systems to standardize operational safety, identify risks in a timely manner and strengthen physical security governance. All Tencent Cloud data centers are sited, constructed or leased in compliance with relevant international standards and local security requirements. At present, Tencent Cloud has deployed two leased data centers in Japan. To ensure the resilience and security of data centers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud has established a robust management system covering data center supplier access, contractual constraints and ongoing supervision. Through annual internal and external audits, Tencent Cloud conducts on-site inspections of operators' data centers to ensure that such facilities meet the information security requirements stipulated by Tencent Cloud. Tencent Cloud requires operators to install smoke detectors, lightning protection and grounding devices, fire alarm and sprinkler systems, power supply systems, shunt circuit systems, fresh air systems, air conditioning systems and temperature monitoring devices at the data centers, and assign personnel to provide round-the-clock maintenance and support for the prompt resolution of equipment failures. Tencent Cloud also requires data center operators to formulate physical security emergency response plans and organize regular safety drills for the data center staff.
P54	Maintenance and Management of Computer-related Equipment	[Basic] Clearly Define Maintenance Methods for Computer-Related Facilities.	Customers shall conduct maintenance inspections on facilities related to the operation of computer systems, including power supply, air conditioning, water supply and drainage, disaster prevention, security, monitoring and wiring systems, and keep records of the inspection details and results. To assist customers in complying with regulatory requirements, Tencent Cloud mandates that data center operators assign personnel to perform regular maintenance on such facilities and provide support for the prompt resolution of equipment failures. Tencent Cloud also requires operators to arrange security staff to conduct strict patrol inspections of all

No.	Domain	Summary of Controls	Tencent Cloud's Response
			computer rooms and equipment in accordance with patrol checklists and schedules, with staff signing and recording the inspection time at each check point.
P55	Maintenance and Management of Computer-related Equipment	[Basic] Confirm Capacity and Usage Status of Computer-Related Facilities.	Customers shall grasp the capacity and performance limits of facilities associated with the operation of computer systems, including power supply, air conditioning, water supply and drainage, disaster prevention, security, monitoring and wiring systems, and monitor their operational status. To ensure the resilience and security of data centers, Tencent Cloud has established a robust management system covering data center supplier access, contractual constraints and ongoing supervision. Tencent Cloud mandates that data center operators monitor and maintain the aforesaid facilities, promptly detect any abnormalities of the facilities and resolve them without delay. Through annual internal and external audits, Tencent Cloud conducts on-site inspections of operators' data centers to ensure that such facilities meet the information security requirements stipulated by Tencent Cloud.
P56	Access Control for Premises/Laboratories	[Basic] Grant Access Rights and Manage Keys.	Customers shall implement access control and key management for critical premises such as data centers and computer rooms. To assist customers in complying with regulatory requirements, Tencent Cloud requires data center operators to formulate stringent access control policies for infrastructure and the physical environment in accordance with regional security requirements of different levels, and establish access control and key management systems.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud mandates that operators install access control systems, establish a complete personnel access control security matrix in the data center access control authorization system based on personnel categories and access permissions, conduct regular reviews of personnel access control permissions, and retain records of the activation or revocation of such permissions, thereby achieving effective control over the access and operation behaviors of all personnel in the data centers. In terms of key management, Tencent Cloud requires operators to formally designate the responsible personnel or departments for the keys of different areas, store the keys in secure and technically segregated locations (such as password-locked safes or locked cabinets), and define clear application and approval procedures for key collection, so as to prevent unauthorized personnel from obtaining the keys. Customers shall manage access to data centers by verifying the eligibility of persons entering and exiting, so as to prevent unauthorized intrusion, the bringing-in of dangerous goods, the unauthorized taking-out of articles and other such acts.
P57	Access Control for Premises/Laboratories	[Basic] Manage Entry/Exit to the Data Center.	To assist customers in complying with regulatory requirements, Tencent Cloud requires operators to establish formal access procedures for physical entry to data centers, verify the identity of persons entering the data centers, and inspect and register the articles they carry. Tencent Cloud mandates that data center operators conduct regular reviews of data center access permissions to ensure the appropriate assignment of such

No.	Domain	Summary of Controls	Tencent Cloud's Response
			permissions and the timely deactivation of access permissions that are no longer relevant or necessary. For external visitors accessing data centers, Tencent Cloud requires operators to establish relevant visitor application and authorization mechanisms, permitting only approved visitors to access designated areas of the data centers at the agreed time and under the accompaniment of relevant staff members.
			Customers shall implement access control for critical rooms such as computer rooms and data storage rooms to prevent unauthorized intrusion, the bringing-in of dangerous goods, the unauthorized taking-out of articles and other such acts. To assist customers in complying with regulatory requirements, Tencent Cloud requires data center operators to formulate stringent access control policies for infrastructure and the physical environment in accordance with regional security requirements of different levels. Tencent Cloud also mandates that operators install access control systems and establish a complete personnel access control security matrix in the data center access control authorization system based on personnel categories and access permissions, thereby achieving effective control over the access and operation behaviors of all personnel in the data centers. In addition, Tencent Cloud requires operators to arrange dedicated staff to accompany personnel entering computer rooms and register the equipment entering and exiting the computer rooms.
P58	Access Control for Premises/Laboratories	[Basic] Manage Entry/Exit to Computer Rooms and Other Critical Areas.	
P59	Access Control for	[Basic] Manage Activities After	Customers shall manage the work and

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Premises/Laboratories	Entry.	activities of persons after they enter critical rooms such as computer rooms and data storage rooms. To assist customers in complying with regulatory requirements, Tencent Cloud requires data center operators to formulate stringent access control policies for infrastructure and the physical environment in accordance with regional security requirements of different levels. Tencent Cloud mandates that operators install access control systems and establish a complete personnel access control security matrix in the data center access control authorization system based on personnel categories and access permissions. In addition, Tencent Cloud requires operators to arrange dedicated staff to accompany personnel entering computer rooms and register the equipment entering and exiting the computer rooms.
P60	Monitoring	[Basic] Establish a Monitoring System for Various Equipment.	Customers shall establish a corresponding monitoring system for the equipment that ensures the normal operation of computer systems (including power supply, air conditioning, water supply and drainage, fire alarm, monitoring and other such equipment), defining clear monitoring objects, monitoring content and monitoring methods. To assist customers in complying with regulatory requirements, Tencent Cloud requires data center operators to monitor and maintain facilities including power supply, air conditioning, water supply and drainage, disaster prevention, security, monitoring and wiring systems, promptly detect any abnormalities of such facilities and resolve them without delay. Through annual internal and external audits,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud conducts on-site inspections of operators' data centers to ensure that such facilities meet the information security requirements stipulated by Tencent Cloud.

5.2.5 Emergency Response

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers shall establish communication procedures to enable prompt and accurate contact with relevant personnel in the event of equipment failures or disasters.
			Tencent Cloud has defined internal and external communication strategies for disaster incidents in its business continuity-related procedures and established multi-channel communication methods, including console announcements, official website notifications, in-site messages, SMS and emails, to timely release incidents that may affect customers.
P70	Response Measures for Failures and Disasters	[Basic] Clarify the communication procedures to stakeholders in case of system failure or disaster.	Tencent Cloud provides a ticket service through the cloud console, supporting customers to report failures, incidents, issues and complaints related to security, availability and confidentiality. Tencent Cloud's ticket system assigns priorities to customer tickets through a tiered response mechanism; when the first-line technical team is unable to resolve an issue effectively, the system will automatically trigger a service escalation process, with the product or technical teams intervening to handle the issue collaboratively, ensuring that customers' needs and feedback receive prompt responses and resolution. Tencent Cloud also provides online and telephone channels on its official website, enabling customers to report problems encountered while using Tencent Cloud services. Tencent Cloud has geographically redundant customer service centers that

No.	Domain	Summary of Controls	Tencent Cloud's Response
			operate 24/7 to handle customer inquiries and requests, delivering high-quality, round-the-clock technical support. In addition, customers can select applicable service plans to access exclusive support, including dedicated support groups, dedicated technical account managers and value-added services. For local support, Tencent Cloud has appointed Information Security Liaisons. The Information Security Liaisons in each region maintain smooth communication with local regulatory authorities and customers in accordance with compliance and business requirements to ensure that Tencent Cloud adheres to legislative, regulatory and contractual obligations.
P71	Response Measures for Failures and Disasters	[Basic] Clarify the communication procedures to stakeholders in case of system failure or disaster.	Customers shall define recovery procedures, namely the steps for restoration after computer systems become inoperable due to failures or disasters, and ensure that such procedures are aligned with emergency response plans. Tencent Cloud builds or leases data centers in multiple locations worldwide in compliance with relevant international standards and local security requirements, offering customers a range of multi-region and multi-availability zone deployment options to meet their business disaster recovery needs and service level requirements. To ensure that customers can respond rapidly and restore critical functions in the event of a cyber security incident, various Tencent Cloud products and services—including computing, networking, storage, database, container and middleware services—are built with high availability features to help customers achieve high

No.	Domain	Summary of Controls	Tencent Cloud's Response
			availability for their systems and services. Examples include: <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, 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>TDSQL-C for MySQL</u>: As a next-generation cloud-native relational database independently developed by Tencent Cloud, it adopts a highly available cluster architecture, which can automatically detect faulty nodes and support second-level failover and recovery. <u>TencentDB for MySQL</u> supports high data reliability and service availability, with a robust mechanism for automatic data backup and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
			In terms of disaster recovery, Tencent Cloud has built a comprehensive business continuity management system and obtained the international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud formulates detailed disaster recovery plans for its cloud products and critical processes, and conducts regular drills in strict accordance with relevant requirements to verify the feasibility of such plans. Tencent Cloud's disaster recovery drills are often carried out by simulating real-world typical disaster recovery scenarios, including offensive and defensive exercises and large-scale failures, to conduct a comprehensive assessment of the system's disaster recovery capability, response speed and recovery capability. For issues identified during drills, Tencent Cloud will implement corrective measures based on the improvement proposals outlined in the drill summary reports, revise the corresponding emergency response plans in a timely manner, and the internal audit department will supervise and inspect the implementation of corrective actions. In addition, Tencent Cloud conducts regular backup and recovery tests to verify data integrity and recoverability, ensuring the storage security and operational reliability of backup data.

No.	Domain	Summary of Controls	Tencent Cloud's Response
P72	Response Measures for Failures and Disasters	[Basic] Investigate and analyze the cause of failures. For cloud-based systems, Financial institutions should confirm with the cloud provider the methods and means for understanding post-failure investigations within their responsibility scope. For cloud usage, financial institutions should consider proactive prevention strategies.	Customers shall investigate failures, document the causes of their occurrence, and prevent the recurrence of similar failures through trend analysis and other such measures. To assist customers in complying with regulatory requirements, in terms of incident response and handling, Tencent Cloud has formulated information security incident management specifications and established an information security reporting, response and handling mechanism along with relevant procedures. Tencent Cloud uses an internal security operation system to record security incidents. For security incidents detected and identified, Tencent Cloud will analyze and classify them based on factors including the nature of the incident, the sensitivity of the involved data and the scope of impact, and promptly notify the corresponding responsible persons to follow up on and handle the incidents. Tencent Cloud is committed to building a proactive defense security capability system covering intelligence, attack and defense, management and planning. By integrating technologies such as threat intelligence, artificial intelligence and big data, it enhances the response capability and efficiency for security incidents. In terms of incident summary and continuous improvement, Tencent Cloud has established a periodic incident analysis mechanism. It conducts regular multi-dimensional analysis of incidents (including incident type, occurrence frequency, scope of impact and severity), and adopts preventive measures based on incident review and root cause analysis to prevent the recurrence of similar incidents. For major security incidents, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
P73	Formulation of Emergency Plans		will set up a dedicated task force to formulate a special analysis report and submit it to the management level for review.
			Customers shall formulate emergency response plans for contingencies such as sudden disasters, accidents, equipment failures or cyberattacks, conduct regular reviews of the plans and update them as necessary. When using cloud services, customers shall develop their emergency response plans in consideration of factors including the activation criteria for such plans and the architectural composition of the systems.
		[Basic] Establish a Contingency Plan.	To ensure the continuous and stable availability of customers' businesses, Tencent Cloud builds or leases data centers in multiple locations worldwide in compliance with relevant international standards and local security requirements, offering customers a range of multi-region and multi-availability zone deployment options.
		For cloud usage, consider: (1) Activation conditions (2) System design (e.g., multi-region/multi-zone architectures)	At present, Tencent Cloud operates two leased data centers with independent power supply and network connections in Japan, which can support customers to store, process and back up data within Japan. Customers can independently and flexibly deploy their data and systems across different regions or availability zones based on their business development needs and data security requirements. Tencent Cloud also formulates differentiated response strategies and business continuity plans based on the results of business impact analyses for its cloud products and services, and develops detailed disaster recovery plans for cloud products and critical business processes. The relevant policies, plans, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. In addition, Tencent Cloud conducts an annual review and update of its business continuity management system, and reviews the business continuity plans and disaster recovery plans for relevant products and services based on business impact analysis results, updating them as required. In accordance with the internal provisions for business continuity management, Tencent Cloud also maintains an emergency response contact list, and designates dedicated personnel to ensure the accuracy and validity of the contact information of all parties included in the list.
P73-1	Formulation of Emergency Plans	[Basic] Establish Incident Response and Contingency Plans for Cyberattacks.	Customers shall formulate incident response plans and emergency response plans specifically for cyberattacks, so as to minimize the scope of damage and business impact, and achieve the earliest possible recovery in the event of significant harm and impaired business operations caused by cyberattacks. To assist customers in complying with regulatory requirements, Tencent Cloud has established a cyber security emergency response plan covering a variety of cyber security emergency scenarios including cyberattacks, malicious programs, data security incidents, equipment and facility failures, and catastrophic events. Based on improving and perfecting the emergency response plan system, supported by the development of an emergency response team, and focusing on standardizing

No.	Domain	Summary of Controls	Tencent Cloud's Response
			emergency response processes, Tencent Cloud continuously enhances its capabilities in monitoring, early warning, notification and disposal, so as to prevent and mitigate the adverse impacts of cyber security incidents. Tencent Cloud conducts regular reviews, updates and tests of its cyber security emergency response plan to ensure its effectiveness.
P74	Backup Site	[Additional] Maintain a Backup Site. For cloud usage, confirm with the cloud provider whether their offering meets the institution's backup requirements. Verification points: (1) Geographic separation between primary and backup zones/regions. (2) Service continuity specifications during disasters.	Customers shall maintain backup sites in different regions based on business priorities. Tencent Cloud operates data centers across multiple regions worldwide, enabling customers to flexibly deploy their data and systems across different regions or availability zones as needed. All Tencent Cloud data centers are sited, constructed or leased in compliance with relevant international standards and local security requirements, and are equipped with highly stable power and air conditioning systems, a complete fire protection system, anti-static facilities and more. Stringent access control policies for infrastructure and the physical environment have also been formulated in accordance with regional security requirements of different levels. At present, Tencent Cloud has two leased data centers with independent power supply and network connections in Japan, which can support customers to store, process and back up data within Japan. Customers can independently and flexibly deploy their data and systems across different regions or availability zones and adopt diverse business continuity models based on their business development needs and data security requirements, so as to meet the disaster recovery requirements of their businesses.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			In addition, to ensure the continuous availability of customers' businesses, various Tencent Cloud products and services—including computing, networking, storage, database, container, middleware and security services—are built with high availability features and supported by corresponding disaster recovery plans.

5.2.6 System Development and Change

No.	Domain	Summary of Controls	Tencent Cloud's Response
P75	System Development and Change Management	[Basic] Clarify System Development and Change Procedures. For third-party libraries, middleware, and hardware used in systems, it is desirable to select secure products provided by vendors who incorporate secure development practices such as "Security by Design" and "Security by Default", to prevent inclusion of backdoors or other unauthorized access routes.	Customers shall define development and change processes to ensure the legitimacy of system development and change content. For third-party libraries, middleware and hardware used in systems, customers shall give priority to selecting secure products provided by vendors that adopt secure development methodologies such as Security by Design and Security by Default. Tencent Cloud offers the following development tools to assist and support customers in development lifecycle management: • <u>Cloud-Native Build (CNB)</u>: Based on the Docker ecosystem, CNB abstracts environments, caches and plugins and adopts a declarative syntax, designed to help developers build software in a more efficient manner. CNB provides a complete developer toolchain with capabilities including code hosting, high-performance R&D pipelines, AI-powered code review, cloud-based development environments, artifact management and custom task sets, enabling effective end-to-end support for the entire R&D process from requirement analysis to deployment and agile development management.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 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. In terms of change management, Tencent Cloud has formulated an internal set of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management standards for product and configuration changes, defining all steps in the change process and the corresponding responsible persons to ensure that all changes undergo proper review, approval and testing prior to implementation. Meanwhile, Tencent Cloud has defined management processes for emergency changes, which may only be implemented upon appropriate approval. In addition, for O&M change operations that may have an impact on customers, Tencent Cloud will promptly issue change notifications to the affected customers through channels such as the official website and in-site messages. For the use of third-party or open-source products, Tencent Cloud has formulated software supply chain security management requirements, specifying that security admission reviews must be conducted when introducing external components, and security hardening and defense measures must be implemented prior to launch to ensure that products pass the pre-launch security inspection. Following product launch, continuous security O&M and inspections will be carried out to resolve security issues in a timely manner. Tencent Cloud will also conduct evaluations of the product's security operation status to identify security risks, urge vendors to make improvements, and review subsequent cooperation strategies with such vendors.
P76	System Development and Change Management	[Basic] Establish a Test Environment. In cases of cloud usage, it is necessary to verify that the cloud provider meets the security standards established by the financial institution. Verification	Customers shall establish a testing environment that does not affect the production environment, and conduct tests related to system development and changes on the premise of not interfering with the production environment. To support customers with cloud-based development, customers may use Cloud-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		points include: (1) Methods or features to securely separate production and test environments in cloud services. Examples: (2) Methods for data and program integration between production and test environments after separation.	<u>Native Build (CNB)</u> to create and utilize development/testing environments. CNB provides cloud-based container environments that can be launched in seconds, equipping developers with the capabilities for coding, compilation, operation and self-testing to support their cloud-based development work. CNB supports users in using either the default development environment or a custom-built one. For isolation requirements, Tencent Cloud also offers <u>Virtual Private Cloud (VPC)</u>, which supports the construction of multiple independent network spaces for the cloud platform resources purchased by customers, and allows for the customization of segment division, IP addresses, routing policies and other configurations. The VPC service is an exclusive cloud-based network space built on Tencent Cloud; based on tunnel technology, it constructs virtual networks over physical networks and leverages virtualization technology to achieve complete internal network isolation between different VPCs, providing customers with independent and isolated secure cloud networks. For Cloud Virtual Machines (CVMs) within a VPC, customers can control the inbound and outbound traffic at the instance and subnet levels by configuring security groups and network ACL rules, thus implementing network access control at different layers. To assist customers in complying with regulatory requirements, Tencent Cloud ensures that the development/testing environment and the production environment are isolated from each other, and prohibits the use of unsensitized production data in the development/testing environment.

No.	Domain	Summary of Controls	Tencent Cloud's Response
P77	System Development and Change Management	[Basic] Clarify Procedures for Production Deployment.	Customers shall define the migration process for the production environment and take into account the characteristics of each system during migration to prevent failures in the migration process. To assist customers in securely migrating their businesses to the cloud, Tencent Cloud provides the Cloud Migration Gateway (CMG) service. As an integrated migration tool and monitoring platform offered by Tencent Cloud, CMG provides official Tencent Cloud migration tools and integrates officially certified third-party migration tools, enabling customers to migrate their systems to the cloud in a convenient and efficient manner. Tencent Cloud conducts stringent evaluations and certifications of the capabilities and migration experience of third-party migration tools to ensure that the solutions and tools selected by customers are all secure and reliable. CMG supports the unified monitoring of all migration tasks, with progress displayed via visual charts, helping customers clearly track the migration progress.
P78	Document Management During Development and Change	[Additional] Clarify Documentation Procedures for Development and Changes.	To properly prepare documents related to development and changes, customers shall define the scope of documents to be prepared and formulate corresponding preparation processes. Customers shall also specify the document storage and management methods for development and change activities, and ensure the proper storage and management of such documents.
P79	Document Management During Development and Change	[Basic] Clarify Documentation Storage and Management Methods for Development and Changes.	To assist customers in complying with regulatory requirements, Tencent Cloud has established relevant procedures and processes for document management. Documents created during the development and change phases are prepared, approved,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			released, used, revised, identified, retained and destroyed in accordance with applicable requirements.
P82	System Decommissioning	[Basic] Formulate a system disposal plan and clarify disposal procedures. When using cloud services, it is necessary to confirm the data decommissioning methods with the cloud service provider for the formulation and implementation of decommissioning plans.	Customers shall formulate system decommissioning plans, define decommissioning procedures, and execute decommissioning only upon obtaining approval. When decommissioning systems, customers shall take measures to prevent information leakage. When using cloud services, it is necessary for customers to confirm the data decommissioning methods with the cloud service provider.
P83	System Decommissioning	[Basic] Implement measures to prevent information leakage during system disposal.	For data deletion and destruction, Tencent Cloud provides a secure and reliable data destruction mechanism. Upon the termination of a customer's services, Tencent Cloud will adopt stringent data erasure methods completely delete all customer data (including replicas and backups) upon the expiration of the retention period; the deleted data shall be irrecoverable. 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 scrapped, Tencent Cloud will promptly conduct complete physical destruction in accordance with rigorous processes.

5.2.7 Measures for Enhancing System Reliability

No.	Domain	Summary of Controls	Tencent Cloud's Response
P84	Hardware Backup	[Additional] Provide backups for main units.	To respond promptly in the event of a failure of primary equipment, customers shall equip core and critical primary equipment of computer systems with spare equipment. Customers shall also provide spare equipment or alternative functions for critical peripheral equipment. For files requiring high reliability, redundancy shall be implemented.
P85	Hardware Backup	The term "peripheral devices" refers to file devices (magnetic disk devices, semiconductor disk devices, magneto-optical disk devices, magnetic tape devices,	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		etc.), console displays, etc.	Tencent Cloud data centers are distributed across multiple regions worldwide, structured into Regions and Availability Zones (AZs), covering mainland China, the Asia-Pacific, North America and Europe. At present, Tencent Cloud has deployed two leased data centers in Japan. Customers can independently and flexibly deploy their data and systems across different Regions or Availability Zones and adopt diverse business continuity models based on their business development needs and data security requirements to meet their business disaster recovery demands. Meanwhile, various Tencent Cloud products are built with high availability features to help customers achieve high availability for their systems and services. Examples include: • <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, which ensures rapid data migration and recovery if any replica malfunctions. • <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. • <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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 Block Storage (CBS)</u> : It adopts a distributed triple-replica mechanism. Its backend data replication mechanism can quickly create a new replica through data migration and other methods in the event of a failure of any single replica, ensuring three available replicas at all times and providing customers with secure and reliable data storage services. CBS data is stored across racks to ensure high reliability. To assist customers in complying with regulatory requirements, Tencent Cloud has designed and implemented a business continuity management framework adapted to its own cloud computing environment, built a comprehensive business continuity management system, and obtained the international standard certification for the ISO/IEC 22301 Business Continuity Management System. To ensure the continuous availability of customers' businesses, Tencent Cloud has implemented redundancy or hot backup mechanisms for hardware devices such as servers, network equipment and security devices, ensuring no data loss and business recoverability in the event of hardware failures. To detect and address hardware device failures or issues in a timely manner, Tencent Cloud manages hardware and other assets through its asset management system, which covers asset registration and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			binding, asset inventory and information update, asset decommissioning and replacement, and other functions, ensuring the stable operation of the underlying cloud platform systems. Tencent Cloud requires the relevant personnel of data center operators to conduct strict daily patrol inspections of all computer rooms and equipment in accordance with patrol checklists and schedules, sign and record the inspection time at each check point, and immediately activate the corresponding response procedures upon detecting infrastructure failures or security incidents. In terms of backup management, Tencent Cloud has formulated backup management procedures. It provides customers with multi-storage replica and backup services based on the functions of its cloud products and services. Tencent Cloud adopts real-time hot backup, redundant storage, remote backup and other methods to ensure the security, reliability and continuous availability of customers' businesses and data on the cloud. For more information related to backup, please refer to the content in Clause 39 Data File Management of Section 5.2.3 in this Guide.
P86	Hardware Backup	[Additional] Provide backups for communication equipment.	To respond promptly to failures of communication equipment, customers shall equip critical communication equipment with spare devices. To safeguard network resilience, Tencent Cloud requires data center operators to ensure that the network egresses of data centers are connected to multiple ISPs, build cross-regional disaster recovery capabilities for the Tencent Cloud network, and effectively mitigate the sustained impacts caused by public network failures of ISPs. The Tencent Cloud underlying network adopts a redundancy architecture;

No.	Domain	Summary of Controls	Tencent Cloud's Response
			combined with traffic engineering scheduling for route-level path priority and route reachability, it ensures that network services are not interrupted by single-point equipment failures. In addition, Tencent Cloud has implemented redundancy and spare parts mechanisms for hardware devices such as network equipment to enable prompt responses to communication equipment failures.
			To respond promptly to line failures, customers shall equip critical lines with backup lines.
			To safeguard network resilience, Tencent Cloud requires data center operators to ensure that the network egresses of data centers are connected to multiple ISPs and provide lines from different ISPs as backups, so as to build cross-regional disaster recovery capabilities for the Tencent Cloud network and effectively mitigate the sustained impacts caused by public network failures of ISPs. The Tencent Cloud underlying network adopts a redundancy architecture; combined with traffic engineering scheduling for route-level path priority and route reachability, it ensures that network services are not interrupted by single-point equipment failures. Tencent Cloud's computing nodes also adopt a redundancy architecture, where a single faulty computing node is automatically and real-time evicted by the scheduler, effectively ensuring the availability of customers' businesses.
P87	Hardware Backup	[Additional] Provide backup lines.	
P89	Measures for Improving Software and Related Quality	[Basic] Incorporate necessary security functions.	Customers shall establish a framework for the implementation of Security by Design, and explicitly incorporate essential security functions during the system planning phase. To assist customers in complying with regulatory requirements, Tencent Cloud has

No.	Domain	Summary of Controls	Tencent Cloud's Response
			developed a set of information system secure development standards, and strived to integrate the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System and ISO/IEC 9001 Quality Management System into the entire product secure development lifecycle (SDLC), covering all stages including requirements, design, R&D, testing, delivery and operation and maintenance. Tencent Cloud involves the security team in each phase of product development to review security requirements, ensuring that cloud products receive robust security control and assessment throughout their lifecycle and mitigating information security and privacy risks. During the requirements analysis phase, Tencent Cloud conducts security analysis of requirements and business risk analysis. The project manager invites relevant teams, such as the testing team and security team, to conduct a security review of the specification of the product requirements, conduct discussions on business content, business processes and technical frameworks, and identify the optimal approach for security integration. Security requirements include, but are not limited to, areas such as identity and access management, data security, network security and security auditing.
P90	Measures for Improving Software and Related Quality	[Basic] Ensuring software quality during the design phase.	Customers shall define the prerequisite requirements for development during the software design phase, and consider reliability design and the standardization of design work to improve the software reliability at the design stage. To assist customers in complying with regulatory requirements, iterative requirements for Tencent Cloud products

No.	Domain	Summary of Controls	Tencent Cloud's Response
			are derived from users, project investors, product brainstorming sessions and operational activities. During the requirements analysis phase, Tencent Cloud conducts security analysis of requirements and business risk analysis. The project manager invites relevant teams, such as the testing team and security team, to conduct a security review of the specification of the product requirements, conduct discussions on business content, business processes and technical frameworks, and identify the optimal approach for security integration. Tencent Cloud analyzes product requirements following formal review. Based on the complexity of the product requirements, the relevant personnel determine whether a detailed technical solution needs to be formulated, which includes overall design, detailed design, implementation plan, testing plan, resource plan and risk management. The project manager invites relevant teams, such as the testing team and security team, to conduct security analysis and technical risk analysis of product design, perform threat modeling for system design, and conduct security technical assessment of the adopted architecture to prevent the implementation of functional modules through insecure methods.
P91	Measures for Improving Software and Related Quality	[Basic] Ensuring quality during the programming phase.	Customers shall conduct programming in accordance with relevant programming specifications, and adopt measures to standardize and automate programming work. For web systems, customers shall take countermeasures against the vulnerabilities of web applications into consideration when building the systems. <u>Cloud-Native Build (CNB)</u> provides a complete developer toolchain with capabilities including code hosting, high-

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated detailed secure coding standards that all internal developers must strictly follow. It also conducts secure programming 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			components, and sensitive information protection.
P92	Measures for Improving Software and Related Quality	[Basic] Ensuring quality during the programming phase.	Customers shall improve software reliability during the testing phase by adopting measures such as formulating test plans, preparing test environments and frameworks, utilizing test support functions, and implementing various management practices throughout the testing phase. To assist customers in complying with regulatory requirements, 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.
p93	Measures for Improving Software and Related Quality	[Basic] Ensuring software reliability considering program distribution.	Customers shall inspect the release environment prior to software launch, verify its integrity and eliminate viruses. To assist customers in complying with regulatory requirements, Tencent Cloud completes software releases in accordance with internally formulated software release standards and processes. When releasing software, Tencent Cloud conducts adaptability testing on physical hardware, operating systems and middleware to ensure the software can run in different

No.	Domain	Summary of Controls	Tencent Cloud's Response
			environments. Meanwhile, Tencent Cloud scans the software for malicious code before its launch to ensure software security. If vulnerabilities are identified, a ticket will be automatically generated and sent to the responsible development team; the team shall fix the vulnerabilities before the software release to prevent security issues from being introduced into the production environment.
P99	Measures for Enhancing Operational Reliability	[Additional] Automate and simplify operations. When using cloud services, financial institutions and similar entities shall confirm with the cloud service provider the functions offered to achieve operational automation and simplification. Examples of such functions are as follows: (1) Set startup timing, interval, conditions, etc., as parameter values for each service provided by the cloud provider; (2) Implement applications that call the cloud provider's management interface and schedule them as jobs in the operations management middleware; (3) Use services provided by the cloud provider for the purpose of operation automation.	Customers shall automate and simplify operations. When using cloud services, customers shall confirm with the cloud service provider the functions offered by the cloud services to achieve operational automation and simplification. Tencent Cloud provides a variety of services to help customers implement operational automation, including: • <u>Cloud API</u>: Cloud API offers interfaces for various resources of Tencent Cloud products. With Cloud API, customers can quickly operate cloud products with only a small amount of code. It features strong compatibility, high ease of automation, and supports remote calls. Customers can freely combine interfaces via Cloud API to call common functions or implement custom function development. • <u>Tencent Infrastructure Automation for Terraform</u>: Based on the plugin extension system of Terraform, a world-renowned IaC tool, this product provides automated capabilities for cloud resource deployment, implementation and management. It is designed to connect the sophisticated and mature infrastructure automation capabilities

No.	Domain	Summary of Controls	Tencent Cloud's Response
			of Terraform with the cloud resource service capabilities of Tencent Cloud, enabling customers to easily implement DevOps, multi-cloud deployment and other models. It is fully compatible with Terraform HCL declarative syntax, supporting the codified description and versioned management of infrastructure cloud resources to improve the efficiency of automated deployment and O&M. • <u>Auto Scaling (AS)</u>: Auto Scaling can automatically detect the health status of instances and dynamically adjust the computing resources of Cloud Virtual Machines (CVMs) based on customers' business needs, policies, and pre-configured scaling conditions. This ensures that a sufficient number of CVM instances are always available to handle the application loads of customers. In addition, a variety of Tencent Cloud storage and database products support automatic data backup functions. For example, <u>TencentDB for MySQL</u> and <u>TencentDB for MongoDB</u> are equipped with comprehensive automatic data backup and lossless recovery mechanisms, and <u>Cloud File Storage (CFS)</u> provides scheduled automatic snapshot functions, among others.
P100	Measures Enhancing Operational Reliability	[Basic] Enhance the Operation Check Functionality. When using cloud services, financial institutions and similar entities shall confirm with the cloud service provider the checking functions available in their operational management services and tools.	Customers shall implement operational check functions to prevent operational errors. When using cloud services, customers shall confirm with the cloud service provider the check functions of the O&M management-related services or tools it offers. Tencent Cloud provides a variety of services to assist customers with

No.	Domain	Summary of Controls	Tencent Cloud's Response
			operational checks and audits, including: • <u>Cloud Log Service (CLS)</u> : CLS is a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. • <u>Cloud Security Center (CSC)</u>: CSC can uniformly collect various cloud security-related data such as alert data from cloud security products, cloud asset configuration change data, cloud user operation behavior data and log data from some cloud products, and provides a unified search and investigation platform to enable customers to achieve comprehensive cloud log auditing, search and investigation. • <u>CloudAudit</u>: It supports supervision, compliance checks, operational reviews and risk audits of Tencent Cloud accounts. With CloudAudit, customers can record logs, conduct real-time monitoring and retain account activities related to operations across the entire Tencent Cloud infrastructure. • <u>Data Security Audit (CDS)</u>: CDS is an AI-powered database security audit system that supports the full-scope audit and storage of all database session information, access operations and SQL statements within an enterprise network. It identifies malicious acts in operations based on multiple rule bases and threat detection engines, and promptly notifies administrators to take corresponding security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			protection measures.
			To assist customers in complying with regulatory requirements, Tencent Cloud has established internal specifications and mechanisms for log collection and management, which govern the recording, extraction, analysis and auditing of log data such as login logs, operation logs and event logs to detect and prevent abnormalities and risks in system activities. In addition, jump servers have been fully deployed in Tencent Cloud's production environment, and all O&M operations in the production environment must be performed through jump servers. O&M operation records are centrally stored on the log platform. Tencent Cloud conducts log audits through O&M security automation audit tools and an internal audit team to mitigate operational risks.
P101	Measures for Enhancing Operational Reliability	[Basic] Enhance Load Monitoring and Control Functions. When using cloud services, financial institutions and similar entities shall confirm with the cloud service provider the availability of load monitoring and traffic control functions. Financial institutions and similar organizations should consider implementing load monitoring and traffic control functions based on such verification.	Customers shall establish an external outsourcing management mechanism/supplier management mechanism, and verify the execution of outsourced services in accordance with outsourcing contracts, agreements and other relevant documents. Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of cloud services and provides real-time monitoring through the management console. To meet customers' outsourcing management requirements, Tencent Cloud
P102	Functions for Early Detection and Recovery	[Basic] Establish System Operation Monitoring Functions. When using cloud services, financial institutions and similar entities shall confirm the scope of responsibilities between the cloud service provider and cloud users	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		regarding the monitoring of system operating status.	<u>Observability Platform (TCOP)</u> supports real-time monitoring, analysis and alerting of cloud products and cloud resources. It can collect and display various monitoring metrics automatically reported by Tencent Cloud products and custom-configured monitoring metrics reported by customers via visual charts, helping customers keep real-time track of the operation status and performance of cloud products. It also supports setting up alerts for metrics and promptly notifying customers of business anomalies through message push and other methods in accordance with the configured alert rules.
		Financial institutions and similar organizations should establish monitoring functions based on such confirmation. If the cloud provider's functions are insufficient, additional tools should be introduced to compensate.	To facilitate customers' convenient capacity planning and adjustment, Tencent Cloud offers <u>Auto Scaling (AS)</u> service. AS can automatically detect the health status of instances and dynamically adjust the computing resources of CVMs based on customers' business needs, policies, and preconfigured scaling-out and scaling-in conditions, ensuring that an adequate number of CVM instances are always available to handle customers' application loads.
			In terms of network traffic monitoring, customers can opt for <u>Flow Logs (FL)</u> to perform real-time, non-intrusive out-of-band collection, storage, and analysis of network traffic, addressing needs such as troubleshooting, architecture optimization, security detection, and compliance auditing.
			In addition, customers can use <u>Cloud Load Balancer (CLB)</u> to enhance reliability. CLB provides secure and efficient Layer 4 and Layer 7 traffic distribution services, which can expand the external service capabilities of application systems through traffic distribution and eliminate single

No.	Domain	Summary of Controls	Tencent Cloud's Response
			points of failure. Adopting a clustered deployment mode, CLB will promptly evict faulty instances to ensure the normal operation of backend server services. To assist customers in complying with regulatory requirements, in terms of device monitoring, Tencent Cloud has deployed an internal network monitoring system to monitor and issue alerts for network devices including routers, firewalls and network servers, and has also implemented Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. In terms of capacity planning and management, Tencent Cloud has formulated a capacity management procedure, specifying that each business department is responsible for the forecasting and planning of the capacity of relevant business systems. Tencent Cloud uses an internal capacity monitoring platform to conduct real-time monitoring of the capacity usage of the underlying supporting services of the cloud platform and identify trends in capacity usage.
P103	Functions for Early Detection and Recovery	[Additional] Provide Failure Detection and Isolation Functions. When using cloud services, financial institutions and similar entities shall confirm with the cloud provider the availability of failure detection and isolation functions.	Customers shall implement fault detection and fault isolation functions to enable rapid fault recovery. When using cloud services, customers shall confirm with the cloud service provider the fault detection and fault isolation functions available, such as log recording capabilities that capture retrospective information about system operations prior to the occurrence of a fault. To facilitate fault detection, Tencent Cloud provides customers with Cloud Log Service (CLS), CLS is a one-stop logging platform that supports log collection,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. CLS allows the configuration of alert policies for one or more log topics; these policies execute monitoring tasks periodically and trigger alert notifications when query and analysis results meet predefined conditions, enabling customers to detect anomalies in a timely manner. Customers may also use Cloud Security Center (CSC) for one-stop security management of cloud assets, including automated asset inventory, detection and identification of various security risks across assets, and automated response and remediation of asset security risks. CSC continuously monitors enterprise security postures, centrally ingests log data from Cloud Firewall, Web Application Firewall, and Host Security, and provides unified auditing, analysis, aggregation, visualization, and tracking of alert logs. Leveraging orchestration capabilities, CSC also supports customers in configuring pre-defined automated remediation and response workflows to improve incident response efficiency. Tencent Cloud also offers Elasticsearch Service (ES), which aggregates and ingests real-time logs from other cloud products such as Cloud Virtual Machines (CVMs) and containers, as well as historical and incremental business data, into Tencent Cloud ES clusters for distributed data storage, query, and analysis. To assist customers in complying with regulatory requirements, Tencent Cloud has established internal specifications and mechanisms for log collection and management, governing the recording,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			extraction, analysis, and auditing of log data including login logs, operation logs, and event logs to detect and mitigate anomalies and risks in system activities. Tencent Cloud conducts log audits through O&M security automation tools and an internal audit team to prevent operational risks. Tencent Cloud has deployed an internal network monitoring system to monitor and issue alerts for network devices such as routers, firewalls, and network servers, and has implemented Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of endpoint assets across all network servers. To enable rapid response and remediation of faults, Tencent Cloud has formulated internal information security incident management specifications and established corresponding reporting, response, and remediation mechanisms and processes. Upon detecting a security incident or receiving a report from other incident discoverers, the Tencent Cloud team immediately activates the response mechanism and initiates multi-dimensional early warning and defense measures. Backed by a 24/7 security operations system, the Tencent Cloud Security Team focuses on core scenarios including vulnerability monitoring, intrusion traceability, and attack mitigation, responding to security alerts in real time, rapidly conducting attack traceability, and formulating emergency remediation plans to effectively contain the spread of security incidents.
P103-1	Functions for Early Detection and	[Additional] Redundant Configurations and Backup Function	For systems configured with redundancy or backup, customers shall take measures to ensure the proper operation of such

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Recovery	Properly.	configurations to enhance system reliability. To assist customers in complying with regulatory requirements, Tencent Cloud has built a comprehensive business continuity management system and obtained the international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud requires its cloud products to adopt a redundancy mechanism across multiple data centers within a single region to ensure the business continuity of cloud services. Tencent Cloud has formulated detailed disaster recovery plans for its cloud products and critical processes, and conducts regular drills in strict accordance with relevant requirements to ensure the timeliness and feasibility of such plans.
P104	Functions for Early Detection and Recovery	[Additional] Provide Degraded Operation and Reconfiguration Functionality During Failures.	In the event of failure, customers shall take prompt measures to address the issue and avoid overall system downtime by scaling back functions or restructuring the system. 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. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated information security incident management specifications, established information security reporting, response and remediation mechanisms and relevant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			processes, and clearly defined the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud uses an internal security operation system to record security incidents. For detected and identified security incidents, Tencent Cloud will conduct analysis and classification based on factors such as incident nature, data sensitivity and scope of impact, and promptly notify the corresponding responsible persons to follow up on and handle the incidents. Backed by a 24/7 security operation system, the Tencent Cloud Security Team focuses on core scenarios including vulnerability monitoring, intrusion traceability and attack mitigation, responds to security alerts in real time, rapidly completes attack traceability and formulates emergency remediation plans, and effectively contains the spread of security incidents. For security incidents that may affect customers, Tencent Cloud will, after internal review and based on the scope and severity of the information security incident, notify customers of the handling and analysis results of the incident through appropriate channels.
P106	Functions for Early Detection and Recovery	[Additional] Implement Recovery Functions for Failures.	Customers shall implement essential recovery functions to enable rapid system restoration and minimize the impact on business operations in the event of a failure. Tencent Cloud builds or leases data centers in multiple locations worldwide in compliance with relevant international standards and local security requirements, offering customers multi-region and multi-availability zone deployment options. Customers can independently and flexibly deploy their data and systems across different regions or availability zones and adopt diverse business continuity models

No.	Domain	Summary of Controls	Tencent Cloud's Response
			based on their business development needs and data security requirements to meet their business disaster recovery demands. Meanwhile, a variety of Tencent Cloud storage and database services are equipped with backup capabilities and support requirements such as multi-redundancy backup and remote disaster recovery. Various Tencent Cloud products and services, including computing, networking, storage, database, container, middleware and security services, are built with high availability features and supported by corresponding disaster recovery plans. In addition, Tencent Cloud has obtained the international certification for the ISO/IEC 22301 Business Continuity Management System and established a comprehensive internal business continuity management system. It conducts regular disaster recovery drills and tests to ensure the disaster recovery capability, response speed and recovery capability of its systems and businesses.

5.2.8 Individual Businesses and Services, Etc.

No.	Domain	Summary of Controls	Tencent Cloud's Response
P145	Remote Work	[Additional] Clarify the management methods for hardware and software used in telework.	Customers shall define management methods for the hardware and software used in remote work and ensure that remote employees are fully informed of the relevant provisions. In this process, customers shall also take data protection and communication protection measures to prevent information leakage during remote work.
P146	Remote Work	[Additional] Implement measures for user authentication and access control in telework.	To facilitate customers to securely and quickly access cloud-based business systems from any location, at any time, and via any mainstream terminal, Tencent Cloud supports SSL VPN remote access technology. SSL VPN protects the security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			of data transmitted over the Internet through encryption and also supports appropriate access control to reduce the occurrence of unauthorized access. Customers can also use VPN Connection to realize the secure transmission of data between on-premises data centers and Tencent Cloud resources. The VPN tunnel encrypts transmitted data using the Internet Key Exchange (IKE) protocol and IPsec, establishing a secure and trusted data tunnel over the Internet to safeguard data security during transmission. The VPN Gateway features high reliability with an underlying active-active architecture, ensuring uninterrupted communication sessions with zero perception by upper-layer applications. To assist customers in complying with regulatory requirements, in terms of mobile device management, Tencent Cloud has formulated relevant specifications for mobile office security management, defining security usage standards for internal mobile devices and information security assurance requirements for mobile office applications. For employees' mobile devices (such as laptops), Tencent Cloud has deployed a zero-trust security management system for security control. Leveraging the system's security capabilities including virus scanning, vulnerability remediation and active defense, it achieves all-round security protection against ransomware, phishing attacks and internal lateral movement. The zero-trust security management system also supports sensitive data exfiltration monitoring, which can audit and block file exfiltration behaviors via email, cloud storage, remote control tools and file transfer tools to prevent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			potential data theft activities.
			In terms of remote access management, Tencent Cloud has established internal procedures for employee remote access management. Employees can only use trusted devices registered on Tencent Cloud to remotely access the Tencent Cloud office network and daily office systems through encrypted communication channels. Tencent Cloud maintains remote access logs to record user operation behaviors. Meanwhile, Tencent Cloud's internal office network is completely isolated from the production environment where customer data is stored. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment of customer data through jump servers. All backend O&M operation records are centrally stored on the log platform and regularly audited by Tencent Cloud's internal audit team.
P150	Artificial Intelligence (AI)	[Additional] Establish Policies and Organizational Framework for AI Use.	Customers shall formulate policies for the use of Artificial Intelligence (AI), defining the corresponding roles and responsibilities, usage standards and requirements, among other provisions, to promote the proper use of AI and fulfill the accountability for the explanation of AI application. Customers shall conduct appropriate governance of AI application, and commit to ensuring its transparency to avoid infringing on the human rights of users or relevant parties, and eliminate inappropriate and harmful bias and discrimination arising from disinformation, misinformation and biased information. Customers shall also adopt AI-related security measures to prevent harm to the life, physical safety, property, mental well-being and the environment of users or
P151	Artificial Intelligence (AI)	[Additional] Define Appropriate AI Operation and Management Methods.	
P152	Artificial Intelligence (AI)	[Additional] Implement Security Measures for AI.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			relevant parties. Tencent Cloud regards the development of Responsible Artificial Intelligence (AI) as one of its long-term strategic priorities. While driving business growth, it is committed to integrating ethics and security into the development and application of AI technologies to foster responsible innovation. Tencent Cloud attaches great importance to the security challenges posed by AI, actively aligns with cutting-edge international trends in AI governance, and continuously elevates its AI governance capabilities to address and mitigate potential risks. On the basis of complying with the laws and regulations of the jurisdictions where it operates, Tencent Cloud takes data quality, security compliance and ethics as key considerations, conducts risk assessments across all stages of the AI lifecycle, and has implemented a series of risk management measures. It also continuously invests R&D resources in areas such as security classification systems, adversarial attack and defense, hidden toxic content detection, training data anonymization, and the integration of social ethics and morality, to support the secure operation of AI products and address emerging data security, model security and ethical risks in the AI field. In terms of data governance, Tencent Cloud fully standardizes and governs the full-lifecycle activities of AI data processing by formulating and implementing data security strategies, and integrates security compliance requirements into the entire AI R&D process. It strictly reviews and screens high-trust data sources, and adopts advanced algorithms for in-depth data cleansing and security filtering, ensuring that AI data is always under effective

No.	Domain	Summary of Controls	Tencent Cloud's Response
			protection and used in a legal manner, thus building a solid defense for user privacy and data security. Meanwhile, regarding issues such as content security, privacy protection and model security, the Tencent Cloud AI Security Team has launched multiple large-scale security tests involving over a thousand participants internally to proactively identify and mitigate AI security risks. In terms of algorithm governance, Tencent Cloud continuously conducts AI algorithm security evaluation and calibration, regularly identifies and fixes potential security vulnerabilities, tests and enhances the anti-attack capabilities of models, optimizes model performance and reduces bias. It has also established a cross-departmental security team review mechanism to ensure that model implementation and data usage comply with business requirements and security standards in all aspects. In terms of operational governance, Tencent Cloud continuously monitors, prevents and responds to risks, and adopts multi-layered security protection to ensure the security and accuracy of model outputs. In addition, it tracks risky content by applying content identification technologies and continuously elevates the security level of models to fulfill its enduring commitment to social and user responsibilities. Tencent Cloud conducts regular disaster recovery drills by simulating real classic disaster recovery scenarios, including adversarial attack and defense and large-scale failures, to comprehensively verify the system's disaster recovery capability, response speed and recovery capability, ensuring that business operations can be rapidly restored to normal in the event of emergencies.

No.	Domain	Summary of Controls	Tencent Cloud's Response
P153	Artificial Intelligence (AI)	[Additional] Conduct Education and Awareness-Raising Regarding AI Use.	Customers shall carry out education and reminder work on AI usage to help users and relevant parties correctly understand AI, and equip them with the knowledge, literacy and ethical concepts required for the proper use of AI. To assist customers in complying with regulatory requirements, Tencent Cloud provides the online Artificial Intelligence(AI) Service Terms on its international official website, which clarifies the relevant rights and liabilities regarding user inputs and AI outputs, usage restrictions on AI products, and limitations of AI products and services. It also offers users feedback channels for submitting complaints or improvement suggestions. In addition, documentation on product introductions and application scenarios of Tencent Cloud AI products and services has been compiled and made available to customers via the official website. Customers can also obtain relevant support through channels including the cloud console, online customer service and telephone hotlines. Tencent Cloud offers a diverse range of products in the field of artificial intelligence and machine learning for customers to choose from, including: • AI Basic Products: Facial Recognition, Automatic Speech Recognition (ASR), Text-to-Speech (TTS), Tencent Machine Translation (TMT), Optical Character Recognition (OCR), Image Creation, Face Fusion. • AI Application Products: eKYC, Tencent Cloud AI Digital Human. • AI Platform Products: Tencent Cloud TI Platform.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• Tencent Cloud Large Models: Tencent Cloud Agent Development Platform

5.3 Equipment Standards

5.3.1 Data Centers

Chapter 6 Equipment Standards of the Guidelines for Computer System Security of Banks and Relevant Financial Institutions focuses on providing standards and requirements for the site selection, design, and construction of data centers of financial institutions. It requires that when planning and constructing data centers, financial institutions shall take into account key elements such as protection measures against natural disasters like earthquakes and tsunamis, fire protection design inside data centers, stability design of power supply management, control of environmental factors such as temperature and humidity, safety of cable layout, protection measures for physical facilities and tenant-exclusive spaces, operability of daily equipment operation and maintenance, as well as compliance of construction site selection and adaptability of design schemes, so as to prevent design omissions from affecting the continuous operation capability of data centers.

To assist customers in complying with regulatory requirements, all Tencent Cloud data centers worldwide are selected, constructed or leased in accordance with relevant international standards and local security requirements. Currently, Tencent Cloud has deployed two leased data centers in Japan. To ensure the resilience and security of data centers, Tencent Cloud has established a rigorous management system covering the entire process from data center supplier admission, agreement constraints to continuous supervision:

- **Supplier Selection Phase:** Tencent Cloud conducts comprehensive due diligence and risk assessment on data center suppliers' physical environment security (e.g., access control, monitoring, fire protection, etc.), information security management systems (e.g., data encryption, access control, etc.) and business continuity assurance capabilities (e.g., disaster recovery plans, fault recovery mechanisms, etc.) by establishing strict supplier security evaluation mechanisms and admission standards, ensuring that selected suppliers meet high security standards.
- **Cooperation Agreement Signing Phase:** Through standardized contract documents, Tencent Cloud and data center operators clearly define the rights and responsibilities of both parties, specify the scope of services provided by data center operators, and quantitatively define core service standards such as service availability levels, providing contractual guarantee for service quality.
- **Data Center Operation Phase:** Tencent Cloud has established a normalized supervision and evaluation mechanism to conduct comprehensive assessments of data center operators' technical capabilities, service response efficiency and risk control effects on a regular basis, ensuring that the core service capabilities provided by Tencent Cloud to customers will not be affected by the risk management defects of data center operators. In addition, in strict accordance with the Service Level Agreement (SLA) signed by both parties, Tencent Cloud requires operators to submit SLA performance reports at agreed intervals. The reports shall cover core contents such as records of major incident handling during the service period,

achievement of key performance indicators, and summaries of maintenance work. Tencent Cloud conducts regular performance evaluations of data center operators, and the results of performance evaluations serve as an important basis for future cooperation with suppliers.

In terms of data center environmental security, Tencent Cloud requires data center operators to employ highly stable, fully redundant power supply and air conditioning systems, among other measures, to avoid the impact of any single point of failure on data center continuity and availability. Tencent Cloud mandates that operators equip data centers with complete fire protection systems, including zoned fire detection systems, automatic fire suppression systems, and manually operated fire extinguishing equipment for emergency use. Tencent Cloud requires operators to install anti-static flooring within data centers and ground equipment such as server racks and cable trays to protect against damage from static electricity. Furthermore, Tencent Cloud requires operators to install systems for lightning protection, radiation protection, power distribution, UPS, lighting, and other facilities necessary for the proper functioning of the computer rooms. It also requires data center maintenance personnel to work in shifts to ensure 24/7 maintenance and rapid resolution of equipment failures.

Additionally, during the site selection phase, Tencent Cloud's data centers in the Japan region fully consider regional geological and meteorological risks. Priority is given to locations with higher elevations, distant from coastlines, and with stable geological structures to mitigate tsunami risks at the source. Through design features such as elevated building foundations and comprehensive drainage systems, the data centers are fortified against flood hazards. The main building structures employ high seismic-resilience designs, comprehensively enhancing earthquake resistance, effectively mitigating seismic risks, and ensuring the continuous and stable operation of the infrastructure.

At present, the data centers in the Japan region have comprehensively obtained multiple internationally authoritative security and privacy compliance certifications. These include certifications from the International Organization for Standardization (ISO) series: ISO/IEC 27001 Information Security Management System certification, ISO/IEC 27017 Cloud Services Information Security certification, ISO/IEC 27018 Public Cloud Personally Identifiable Information (PII) Protection certification, ISO/IEC 27701 Privacy Information Management System certification, and ISO/IEC 29151 Personally Identifiable Information Protection certification. Additionally, they have passed the Cloud Security Alliance (CSA) STAR Security, Trust, Assurance, and Risk certification, the Payment Card Industry Data Security Standard (PCI-DSS) International Public Cloud certification, and SOC Type 2 audits. This establishes a comprehensive, multi-dimensional compliance system covering information security, privacy protection, cloud service compliance, and payment data security, strictly adhering to international best practices and industry high-standard control requirements.

5.4 Audit Standards

5.4.1 System Audit

No.	Domain	Summary of Controls	Tencent Cloud's Response
A1	System Audit	[Basic] Establish a System Audit Framework.	Customers shall establish a system related to system audits and select audit methods to

No.	Domain	Summary of Controls	Tencent Cloud's Response
A1-1	System Audit	[Basic] Conduct Internal Audits Focused on Cybersecurity.	monitor and evaluate the management of computer systems. They shall also formulate internal audit plans concerning cybersecurity, conduct internal audits focusing on cybersecurity, and accurately track the rectification progress of issues identified in the audits. To support customers' audit and review requirements, Tencent Cloud can assign dedicated personnel to provide assistance and actively respond to audit or review initiatives launched by customers. Meanwhile, the Tencent Cloud Security Team continuously monitors and assesses internal security risks to ensure the effectiveness and reliability of the information security management system. The team conducts internal security audits at least once a year and maintains continuous monitoring of cloud platforms and internal systems, ensuring that they maintain a robust security posture and comply with the provisions and requirements of relevant laws, regulations, and security management standards. In addition, Tencent Cloud undergoes professional audits by independent third parties annually and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory authorities, company shareholders, and other relevant stakeholders by providing attestation - based System and Organization Controls (SOC) reports. Specifically for the Japanese region, Tencent Cloud has assessed its current control status in accordance with the FISC Security Guidelines on Computer Systems for Financial Institutions and formulated corresponding System and Organization Controls (SOC) reports on this basis. These

No.	Domain	Summary of Controls	Tencent Cloud's Response
			reports cover control points related to the security, availability, and confidentiality of the Tencent Cloud platform, so as to demonstrate that Tencent Cloud's relevant measures meet the required standards. For issues identified in audits, Tencent Cloud will assess their potential impact on customers, conduct in - depth analysis of the root causes of such issues, and formulate and implement corresponding rectification measures accordingly. If relevant issues may affect the business operations or data security of financial institution customers, Tencent Cloud will promptly notify the affected financial institutions. Meanwhile, the senior management will conduct regular follow - ups and continuous monitoring on the implementation of rectification plans and specific actions to ensure that the issues are effectively resolved.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Cybersecurity for the Financial Sector

Based on the results of past inspections and monitoring of financial institutions, as well as changes in the internal and external landscape of the financial industry, the Financial Services Agency (FSA) of Japan issued the Guidelines on Cybersecurity in the Financial Sector on October 4, 2024, aiming to continuously elevate the overall cybersecurity level of the financial sector. From a cybersecurity perspective, the guidelines clarify the "basic response requirements" and "recommended response requirements" that financial institutions and similar entities shall fulfill, covering such aspects as governance, identification, protection, detection, response, recovery, and third-party risk management.

Among these, the "basic response requirements" refer to the fundamental obligations that all financial institutions are generally required to implement. The "recommended response requirements" refer to the measures suggested for implementation in financial institutions whose incidents may exert significant impacts on regional social and economic activities (taking into account factors such as the scale and characteristics of the institutions), as well as the good practices to be referred to and the advanced experiences obtained through dialogues with regulatory authorities or financial institutions of other countries. Japan's FSA requires financial institutions and similar entities to identify and assess cybersecurity risks on the basis of their own operating environment, business strategies, and risk appetite, and adopt security measures commensurate with the identified risks.

In this chapter, Tencent Cloud will refine and summarize the control requirements relevant to cloud service providers as specified in the Guidelines on Cybersecurity in the Financial Sector, and elaborate on how Tencent Cloud, as a cloud service provider, can assist financial institutions and similar entities in complying with the relevant requirements.

6.1 Establishment of Cybersecurity Management System

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.1.1	Establishment of Basic Policies and Regulations	[Basic Response Measures]:	Customers shall formulate basic policies, relevant strategies and implementation plans for cybersecurity management, improve the corresponding organizational structure, and establish a cybersecurity management system. They shall conduct regular reviews of the cybersecurity management system and engage external experts to validate cybersecurity governance. Customers shall actively advance various measures to ensure cybersecurity, integrate cybersecurity risks into the risk management framework, and foster an organizational culture that prioritizes cybersecurity. They shall also establish mechanisms for the collection and analysis of early warning information,
		①The Board of Directors and similar bodies shall treat cybersecurity risks as part of the organization's overall risk management and establish a fundamental policy for cybersecurity management.	
		②The Board of Directors and similar bodies shall recognize the importance of ensuring cybersecurity for the organization's strategic objectives,, and taking into account requirements from stakeholders and the internal and external environment, including laws and regulations, to establish	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the necessary cybersecurity management posture. Furthermore, they shall review the cybersecurity management posture at least once a year.	monitoring mechanisms, and crisis management mechanisms against cyberattacks.
		③ Senior management shall establish cybersecurity management posture.	To assist customers in complying with regulatory guidelines, in terms of information security management policies, 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 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. Tencent Cloud is certified against internationally recognized standards, including: • ISO/IEC 27001 – Information Security Management System. • ISO/IEC 27017 – Cloud Service Information Security Management. • ISO/IEC 22301 – Business Continuity Management. ISO/IEC 20000 – IT Service
		④ Senior management shall formulate cybersecurity-related strategies and action plans (including multi-year plans), ensuring the effectiveness and adequacy of these action plans.	
		⑤ Senior management shall simultaneously promote initiatives to ensure cybersecurity, including Security by Design.	
		⑥ Senior management shall take the lead in fostering an organizational culture that ensures cybersecurity.	
		⑦ Senior management shall clearly define the roles, responsibilities, and authorities of the cybersecurity responsible department and relevant parties.	
		⑧ Senior management shall request the responsible departments and similar entities to submit the following reports at least once a year: The status of cybersecurity risks facing the organization; The results of cybersecurity risk assessments; The progress of action plans.	
		⑨ Senior management shall continuously improve the cybersecurity management posture.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		[Desirable Response Measures]	Management.
		a. To ensure governance concerning cybersecurity, which is an important prerequisite for management to make appropriate business decisions, arrangements should be made to utilize sufficient cybersecurity knowledge (including the use of external experts). b. The Board of Directors and similar bodies shall position cybersecurity risk as part of integrated risk management and set risk appetite and risk tolerance. c. Where possible, senior management shall publicly disclose the content of their organization's cybersecurity initiatives to demonstrate their significance to both internal and external stakeholders, while carefully considering the potential to encourage attacks by adversaries. d. Senior management shall request the responsible departments and similar entities to submit the following reports at least twice a year: Cybersecurity-related performance indicators (KPIs) and risk indicators (KRIs) e. Senior management shall appoint an individual with sufficient knowledge and experience in cybersecurity as the responsible person (such as a CISO) for centrally managing cybersecurity within the organization, who holds a position allowing regular direct reporting to	In terms of the information security management organizational structure, Tencent Cloud has established a dedicated security governance framework, defining roles and responsibilities across different levels and setting mechanisms for security audits and risk assessments. Tencent has formed a Security Technology Committee and specialized security teams across various domains. Additionally, Tencent Cloud maintains robust HR management standards and procedures to ensure personnel are recruited and assigned according to role requirements. Tencent Cloud brings together industry-leading security experts to deliver secure, reliable, professional, and compliant products and services. Tencent Cloud has also built a robust internal information security training mechanism, requiring regular employees, consultants, interns and outsourced employees to complete information security training courses. Tencent Cloud consistently integrates information security management into daily management work to ensure that all employees understand and comply with the internal information security management policies and requirements. In terms of security audit and assessment, the Tencent Cloud Security Team conducts an internal security audit at least once a year to ensure compliance with the provisions and requirements of relevant laws, regulations and security management standards. Tencent Cloud also undergoes regular professional audits by independent third parties, and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory

No.	Domain	Summary of Controls	Tencent Cloud's Response
		senior management, and shall establish a relationship enabling direct communication with top management during both normal operations and emergencies.	authorities, company shareholders and other relevant stakeholders by providing attestation-level System and Organization Controls (SOC) reports. In terms of risk management, Tencent Cloud develops and maintains an internal risk management framework with reference to standards including ISO/IEC 27001:2022, ISO/IEC 27018:2014, MTCS and CSA-Star to identify, analyze and manage identified risks. Tencent Cloud conducts a risk assessment regularly, identifying risks based on the results of process analysis of risk scenarios, business products or services. For the identified risks, Tencent Cloud assesses the likelihood and impact of each risk, classifies risk levels, takes corresponding follow-up actions, and maintains formal records thereof. Tencent Cloud also continuously follows up on risk mitigation progress, assesses residual risks, and ensures that the relevant responsible persons have properly managed risks in accordance with Tencent Cloud's risk management requirements. In addition, Tencent Cloud maintains and revises risk assessment methodologies and risk registers in light of the evolving trends in the cloud industry and internal management practices. Furthermore, Tencent Cloud has formulated crisis management procedures, which clearly define the crisis management processes and the relevant responsible teams in the event of emergencies or disasters affecting Tencent Cloud's business products or services.
2.1.2	Establishment of Regulations and Business Processes	[Basic Response Measures] ① Senior management shall establish regulations and business processes related to cybersecurity	Customers shall formulate rules, regulations and business processes related to cybersecurity, including those for information asset management, risk assessment, vulnerability management,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and review them at least once a year.	penetration testing, access control, education and training, data management, log management, security design, incident response and recovery, and third-party risk management, and conduct reviews and revisions at least once a year. Customers shall also establish reporting and communication mechanisms and relevant channels to address cybersecurity risks including those from third parties.
		② Senior management shall establish cross-organizational reporting, communication, consultation routes, and command structures for cybersecurity risks, including those arising from third parties.	In terms of rules, regulations and business processes, Tencent Cloud has established an information security management system, and conducts regular reviews and updates of relevant systems and processes on an annual basis to ensure that the control objectives, control procedures and control measures of the management system comply with relevant security policies, standards, procedures and legal requirements. Tencent Cloud has obtained international security-related standard certifications including the ISO/IEC 27001 Information Security Management System, ISO/IEC 27017 Cloud Services Information Security Management System, ISO/IEC 22301 Business Continuity Management System, and ISO/IEC 20000 IT Service Management System. In terms of communication and liaison with customers, Tencent Cloud has established a variety of communication channels to facilitate communication between Tencent Cloud and its external customers, such as the cloud console, email and dedicated hotlines. The Tencent Cloud console provides a ticketing service, supporting customers to report faults, incidents, issues and complaints related to security, availability and confidentiality. Customers may also select applicable

No.	Domain	Summary of Controls	Tencent Cloud's Response
			service plans to obtain exclusive support including dedicated support groups, dedicated technical account managers and value-added services.
2.1.3	Securing Management Resources and Developing Talent	[Basic Response Measures] ① Senior management shall allocate appropriate resources by assigning personnel with specialized expertise to the cybersecurity responsible department and similar units, and by allocating necessary budgets. ② Senior management shall formulate plans for developing and securing talent in alignment with the fundamental policy for cybersecurity management ③ Senior management shall actively participate in training and exercises to acquire the skills and know-how necessary to support governance of cybersecurity by management and to foster an organizational culture aimed at ensuring cybersecurity. ④ Regarding talent development, the following types of personnel should be systematically secured, including through the utilization of external talent.	Customers shall assign professionals with specialized competencies to the cybersecurity accountability department and other relevant departments, formulate sustainable talent recruitment and development plans (including cybersecurity-related knowledge training for management personnel), and provide appropriate resource support to ensure a diversified talent pool in a planned manner. The operation procedures, user manuals and other documentation for Tencent Cloud products have been formalized and are available to customers via the official website. Tencent Cloud also provides customers with Tencent Cloud training and certification programs based on Tencent Cloud product knowledge and relevant professional capabilities, so as to enhance customers' technical proficiency and cloud service competency. In addition, Tencent Cloud offers customers multiple support channels, including 24/7 ticketing service, 24/7 hotline, intelligent customer service and self-service, to continuously address customer inquiries and feedback. Tencent Cloud's customer service team and technical experts will provide customers with prompt and effective support. To assist customers in complying with regulatory guidelines, Tencent has established a Security Technology Committee and specialized security teams with distinct functions and expertise across various domains, and assembled a team of industry veteran experts dedicated to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			delivering secure, reliable, professional and compliant products and services to customers. Tencent Cloud has formulated a comprehensive set of human resource management standards and procedures internally to ensure the recruitment and deployment of personnel in accordance with job requirements. During the recruitment process, Tencent Cloud conducts due diligence on candidate employees, including verification of academic qualifications and professional certification credentials. It has also brought together a team of seasoned industry experts to provide customers with secure, reliable, professional and compliance-aligned security products and services. In addition, Tencent Cloud has designed diverse career development paths for its employees, equipped them with abundant and high-quality learning resources, and continuously optimized its training courses and systems to support employees' personal growth and career advancement.
2.1.5	Internal Audit	[Basic Response Measures]: ① The internal audit department shall, as necessary utilizing external experts, establish an internal audit plan for cybersecurity based on a risk-based approach and conduct internal audits focusing on cybersecurity (including the establishment, operation, incident response and recovery, compliance with laws and regulations, and third-party risk management) from an independent standpoint. ② The internal audit department shall promptly report significant findings from internal audits to the Representative Director and the	Customers shall formulate an internal audit plan for cybersecurity from an independent standpoint in accordance with a risk-based approach and engage external experts when necessary to conduct internal cybersecurity audits. For major issues identified in internal audits and the corresponding rectification progress, customers shall promptly report to the senior management. In addition, customers shall assign personnel with adequate cybersecurity knowledge and professional competencies to the internal audit department. To assist customers in complying with regulatory guidelines, the Tencent Cloud Security Team continuously monitors and assesses internal security risks to ensure the effectiveness and reliability of the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Board of Directors and similar bodies, and accurately track the status of improvements for identified issues. [Desirable Response Measures]: a. Assign personnel with appropriate knowledge and expertise in cybersecurity to the internal audit department.	information security management system. The team conducts an internal security audit at least once a year and keeps a constant watch on the cloud platform and internal systems to maintain a robust security posture and ensure compliance with the provisions and requirements of relevant laws, regulations and security management standards. Furthermore, Tencent Cloud undergoes annual professional audits by independent third parties and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory authorities, company shareholders and other relevant stakeholders by providing attestation-level System and Organization Controls (SOC) reports. For non-conformities identified in audits, Tencent Cloud will promptly analyze the actual or potential causes leading to such non-conformities, assess the need and priority for implementing corrective and preventive actions, and execute such actions upon obtaining relevant approvals. The implementation effectiveness of corrective actions is continuously tracked and documented. In addition, regarding customer audits and regulatory reviews, Tencent Cloud will, based on actual circumstances and the agreements and commitments with customers, cooperate with customers' third-party security audits and supervision, provide dedicated personnel for assistance, and actively respond to and cooperate with audit activities initiated by customers.

6.2 Identification of Cybersecurity Risks

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.2.1	Information Asset Management	2.2.1[Basic Response Measures]	Customers shall formulate information asset lifecycle management procedures, and classify and protect information assets based on their confidentiality, integrity and availability. Customers shall establish ledgers for information systems, external system services, hardware, software and data, and formulate corresponding maintenance procedures.
		① Establish procedures, etc., for managing information assets according to their lifecycle (acquisition, use, storage, disposal), and review them as necessary.	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.
		② Classify and manage information assets according to their level of importance (confidentiality, integrity, availability) to determine protection priorities.	
		2.2.1.1 Information Systems and External System Services	
		[Basic Response Measures]	
2.2.1	Information Asset Management	① Establish registers, etc., to appropriately manage information systems and external system services, define maintenance procedures, and ensure comprehensive awareness of their current status. This includes information systems managed by each department.	In terms of data asset management , The <u>Data Security Governance Center (DSGC)</u> helps customers automatically identify and classify cloud-based data assets and assess associated security risks.
		2.2.1.2. Hardware, Software, etc.	
		[Basic Response Measures]	
		① Establish procedures, registers, etc., to appropriately manage hardware, software, and other assets. Define maintenance procedures to ensure comprehensive awareness of their current status.	
		[Desirable Response Measures]	
2.2.1	Information Asset Management	a. Include multifunction devices and dedicated-purpose devices in the scope of management via	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		registers, etc. b. Where necessary, also include assets of third parties within the management scope. c. When classifying information assets related to hardware and software, ensure risk management can be conducted considering the dependency of critical operations on third parties. d. Identify information assets such as personally owned devices not under management and the use of unauthorized cloud services (Shadow IT, etc.), and respond appropriately e. Establish a Software Bill of Materials (SBOM) for the following: Software developed in-house; Services in use. 2.2.1.3. Information (Data) [Basic Response Measures] ① Establish registers, etc., to appropriately manage customer information and confidential information, define maintenance procedures, and ensure comprehensive awareness of their current status..	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 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 assist customers in complying with regulatory guidelines, Tencent Cloud has formulated internal information asset management specifications and full-lifecycle management processes, and conducts classified and graded management and protection of assets such as electronic data, hardware and its 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., to ensure the stable operation of the underlying cloud platform and provide reliable support for business systems.
2.2.2	Risk Management	2.2.2.1. Collection and Analysis of	Customers shall collect threat and

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Process	Threat and Vulnerability Information [Basic Response Measures]: ① Collect threat information and vulnerability information related to cyberattacks from public agencies, information sharing organizations, and third parties, in addition to the organization's own threat information. ② Organize and analyze the collected information, and evaluate the impact these threats and vulnerabilities may have on the organization's operations and information assets. ③ Review the sources of information collection and the methods of collection and analysis at least once a year, and make necessary improvements. [Desirable Response Measures]: a. Actively participate in specialized information-sharing activities such as financial ISACs, cross-industry groups, and international organizations, relevant to the organization's business, to collect and share threat and vulnerability information. b. When conducting threat analysis, include severe but plausible cyberattack scenarios, even if they have not occurred in the past. c. Pay attention to the organization's surrounding environment, such as new technologies (AI, quantum computers, etc.), geopolitical	vulnerability information related to cyberattacks from the organization itself, as well as public institutions, information sharing organizations and third parties, collate and analyze the collected information, and assess the potential impact of such threats and vulnerabilities on the organization's business and information assets. Customers shall also actively participate in threat information sharing activities organized by highly professional organizations, cross-industry groups and international organizations, and pay attention to external environmental changes affecting the organization such as new technologies, geopolitical developments, disinformation and industry trends when collecting information. Customers shall review the collection sources, methods and analysis methods of threat and vulnerability information at least once a year and make improvements as needed. 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		trends, disinformation, and industry trends, when collecting information.	In addition, with SaaS as its core, TIX supports multiple delivery methods including web-based API, SDK, TIP and mini programs to meet the diverse needs of customers. TIX can also be integrated with customers' existing security protection products to link cloud-based intelligence data with such products, thereby improving the overall efficiency of security operations and threat response. Empowered and supported by TIX, Tencent Cloud is committed to building a proactive defense security capability system of "Intelligence - Offense and Defense - Management - Planning". By integrating threat intelligence, artificial intelligence, big data and other technologies, Tencent Cloud enhances the response capability and efficiency of security incidents, and has established a 24/7 Security Operations Center that focuses on threat detection, investigation and response to achieve the visibility, comprehensibility and controllability of security postures.
		2.2.2.2. Risk Identification and Assessment [Basic Response Measures] ① Establish procedures for identifying and assessing cybersecurity risks. ② Assess cybersecurity risks at least once a year, based on the likelihood of cyberattacks (considering threat and vulnerability information) and the potential impact on the organization's operations and information assets if an attack occurs. Also conduct assessments when significant threats or vulnerabilities are identified, or	Customers shall establish processes for cybersecurity risk identification and assessment, and conduct cybersecurity risk assessments on a regular basis (at least once a year), as well as when major threats or vulnerabilities are identified, or new products or services are launched. When conducting risk assessments, customers shall identify critical business operations, take into account the internal personnel, equipment and systems required to sustain such operations and the level of reliance on third parties, and identify organizational vulnerabilities through scenario analysis, tabletop exercises, stress tests and other methods. Customers shall prioritize risks based on risk assessment results and formulate risk response plans. In light of the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		when launching new products or services. ③ When conducting risk assessments, consider risks such as the breach of perimeter defense security and insider threats, and include risks to systems located within internal network segments. [Desirable Response Measures] a. When conducting risk assessments, identify critical operations and consider the interdependencies among personnel, equipment, systems, and third parties within the organization necessary to maintain these critical operations. b. When conducting risk assessments, identify organizational vulnerabilities and consider potential impacts on critical systems and operations through scenario analysis, tabletop exercises, or stress testing. Consider diverse scenarios that are severe but plausible. 2.2.2.3. Risk Response [Basic Response Measures] ① Based on the results of risk assessments, prioritize risks and develop a risk response plan. ② Establish procedures for handling exceptions and risk acceptance in risk response.. ③ Report the risk response plan. 2.2.2.4. Continuous Improvement Activities [Basic Response Measures]	recommendations, findings, issues and lessons learned from exercises and training, vulnerability detection, penetration testing, audits, risk assessments and actual incidents, customers shall implement improvements in accordance with relevant procedures. In addition, customers shall evaluate the effectiveness of the cybersecurity risk management system, risk assessment processes, and monitoring and detection-related procedures at least once a year and carry out continuous improvements. To assist customers in risk assessment and management, Tencent Cloud provides the Cloud Security Center (CSC). CSC enables one-stop security management of cloud assets, including automated asset inventory, detection and identification of various security risks to assets, and automated response and remediation of asset security risks. It supports periodic detection of six major categories of risks: port risks, vulnerability risks, weak password risks, content risks, cloud resource configuration risks and service exposure risks, and continuously monitors enterprise security status. It also centrally ingests log data from Cloud Firewall, Web Application Firewall and Host Security, and provides unified auditing, analysis, aggregation, visualization and tracking of alert logs. In addition, leveraging orchestration capabilities, CSC allows customers to preconfigure automated remediation and response workflows to enhance threat response efficiency. Customers may also opt for the Cloud Performance Testing Service (PTS), which verifies system availability and stability in an all-round manner by simulating real business scenarios with a

No.	Domain	Summary of Controls	Tencent Cloud's Response
		① Evaluate the process for cybersecurity risk assessment at least once a year according to changes in the internal and external environment, and implement continuous improvement activities. ② Evaluate the effectiveness of the establishment and operation of the cybersecurity risk management posture at least once a year and make improvements. ③ Implement improvements based on recommendations, findings, and lessons learned from exercises and training, vulnerability assessments and penetration testing, audits, risk assessments, and actual incidents, in accordance with relevant procedures. [Desirable Response Measures] a. Evaluate and improve procedures related to monitoring and detection at least once a year, in response to changes in the threat landscape, technological advancements, and lessons learned. b. Establish a system to measure and evaluate performance indicators (KPIs) and risk indicators (KRIs) and report them to senior management. Set specific goals and targets to identify improvement status and challenges.	massive number of users. PTS offers the capability to generate millions of concurrent requests across multiple regions, along with features such as traffic recording, scenario orchestration, customized traffic generation and advanced script customization. It enables rapid definition of pressure test scenarios based on business models and realistic replication of large-scale business access scenarios for applications, helping customers proactively identify application performance issues. To assist customers in complying with regulatory guidelines, Tencent Cloud has formulated an internal information security risk management procedure, which clearly defines and provides guidance on the work content of the entire risk management process, including risk identification, risk analysis, formulation of risk remediation plans, and risk tracking and monitoring. • Risk Identification: Tencent Cloud conducts a risk assessment regularly. It identifies risk scenarios applicable to Tencent Cloud from sources such as industry security incident reports, Tencent Cloud's practical experience and risk databases of professional institutions, and further identifies risks based on the results of process analysis of such risk scenarios, business products and services. • Risk Assessment: Tencent Cloud assesses asset value, the likelihood of risks occurring in identified scenarios and the severity of potential impacts, and calculates the risk level for each identified risk. • Risk Remediation: Based on risk analysis results, Tencent Cloud adopts corresponding response

No.	Domain	Summary of Controls	Tencent Cloud's Response
			strategies and mitigation measures for identified risks. For high-level risks, the risk owner formulates a risk remediation plan (including risk transfer or risk reduction measures) and updates the risk management register; for medium-level risks, the risk owner determines whether a risk remediation plan is required based on actual circumstances; low-level risks are deemed acceptable risks. Tencent Cloud conducts a review of residual risks at least once a year to monitor their status and risk values. • Risk Monitoring, Review and Reporting: Tencent Cloud compiles the results of risk assessments, issues a risk assessment report and submits it to the management. It also maintains a risk management register to monitor changes in risk conditions and the status of risk remediation plans, and adjusts the risk management plan in real time as needed. In addition, Tencent Cloud has defined key risk indicators (KRIs), measures such indicators on a regular basis, analyzes the root causes of identified issues against acceptable risk criteria, and proposes targeted improvement recommendations and solutions.
2.2.3	Vulnerability Management for Hardware, Software, etc.	[Basic Response Measures] ① Establish procedures, etc., for vulnerability management of hardware, software, and other components, and review them as necessary. ② Based on the established procedures for hardware and software vulnerability	Customers shall establish procedures for hardware and software vulnerability management, assess the obtained vulnerability information, and adopt and manage response measures based on system importance and the severity of risks or vulnerabilities. Customers shall set up relevant approval procedures for exceptional cases where no response measures are implemented. For high-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management, determine whether action is required for acquired vulnerability information. ③ Set response deadlines (e.g., for patch application) based on system criticality, risk level, or vulnerability severity, and manage response records. ④ When a high-severity vulnerability is identified, promptly identify affected information systems, etc., based on registers, etc., for information systems and hardware/software, and respond promptly. ⑤ For high-severity vulnerabilities, include systems owned by group companies and overseas locations within the scope of vulnerability response. ⑥ For high-severity vulnerabilities, manage vulnerability responses for systems owned by important third parties (including shared-use systems). In managing these, consider utilizing reports from third-party attestation (e.g., SOC 2) or contractual documents.	severity vulnerabilities, customers shall manage the vulnerability response measures for systems owned by third parties such as cloud service providers. In the management process, consideration may be given to using documents such as third-party assurance reports (e.g., SOC 2 reports) or contracts. To assist customers in vulnerability and risk management, Tencent Cloud provides the Cloud Security Center (CSC). CSC enables one-stop security management of cloud assets, including automated asset inventory, detection and identification of various security risks to assets, and automated response and remediation of asset security risks. Leveraging Tencent's intelligence capabilities, CSC can push the latest vulnerabilities to customers and provide detailed vulnerability reports, including the scope of vulnerability impact and remediation recommendations, helping customers achieve timely awareness and rapid remediation of high-risk vulnerabilities. In addition, CSC uses orchestration capabilities to support customers in preconfiguring automated remediation and response workflows to improve threat response efficiency. To assist customers in complying with regulatory guidelines, Tencent Cloud has established relevant procedures for threat and vulnerability management to promptly identify and take measures to mitigate or remediate threats and vulnerabilities facing information systems. Tencent Cloud conducts regular vulnerability scanning and penetration testing on information systems; during the testing process, past threats and vulnerabilities are reviewed, and the remediation status of vulnerabilities is verified through repeated testing. Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			risks identified during scanning or testing are notified to relevant departments via security tickets for assessment and follow-up. If an assessment finds that a vulnerability may impact customers' business operations, Tencent Cloud will promptly notify customers of vulnerability-related information through official website announcements and in-site messages. The notification content includes, but is not limited to, a vulnerability description, the scope and severity of the impact, the control measures Tencent Cloud has adopted, and targeted remediation recommendations and specific operational guidelines for customers. In addition, Tencent Cloud undergoes regular professional audits by independent third parties and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory authorities, company shareholders and other relevant stakeholders by providing attestation-level System and Organization Controls (SOC) reports. Specifically for the Japan region, Tencent Cloud assesses its current control status in accordance with the *FISC Security Guidelines for Computer Systems of Financial Institutions, etc.*, and compiles corresponding SOC reports on this basis, covering control points related to the security, availability and confidentiality of the Tencent Cloud platform.
2.2.4	Vulnerability Assessment and Penetration Testing	[Basic Response Measures] ① Regularly conduct vulnerability assessments and penetration testing, considering the level of risk and the criticality of systems, to identify vulnerabilities and security issues and drive improvements. Establish relevant	Customers shall establish procedures for vulnerability detection and penetration testing, conduct such tests on a regular basis, prioritize the issues identified, define corresponding response measures and timelines, and follow up on the implementation of these measures. In terms of penetration testing, Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
		procedures, etc., and review them as necessary. [Desirable Response Measures] a. Include VPN networks and internal environments that are not directly connected to the internet within the scope of vulnerability assessments and penetration testing. b. Periodically conduct Threat-Led Penetration Testing (TLPT). c. For improvements addressing issues identified through exercises and training, either conduct follow-up exercises to verify their effectiveness, or obtain approval from senior management, etc., for accepting the residual risk. d. Implement combined exercises and training by integrating various types (e.g., internal exercises, vendor-provided training, industry-specific exercises, regulator-hosted drills) considering their respective scale and characteristics.	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. To assist customers in complying with regulatory requirements, Tencent Cloud has established an internal regular vulnerability scanning and penetration testing mechanism. Internal vulnerability scanning of Tencent Cloud typically covers web vulnerabilities, component vulnerabilities, configuration scanning, etc. It uses a

No.	Domain	Summary of Controls	Tencent Cloud's Response
			vulnerability scanning system to automatically generate scanning tasks for vulnerability detection of assets in the cloud environment, followed by the analysis, classification and remediation of detected vulnerabilities. In terms of penetration testing, the Tencent Cloud Security Team conducts regular full-link large-scale penetration tests, and flexibly carries out targeted penetration tests before the launch of new products or in the event of major changes. Test results are notified to the relevant responsible departments through security work orders, which shall promptly perform vulnerability remediation or implement other compensating control measures to ensure that exploitable vulnerabilities identified in penetration tests are properly addressed. In addition, Tencent Cloud regularly conducts red-blue team exercises to simulate and defend against cyberattacks in real - world scenarios.
2.2.5	Exercises and Training	[Basic Response Measures] ① Conduct regular exercises and training to verify the effectiveness of the organization's cyber incident response plan and contingency plan, identify challenges, and drive continuous improvement (including participation in exercises and training hosted by other organizations). Where necessary, consider involving external service providers in the exercises/training and participate in cross-industry exercises. ② Senior management, the person responsible for overall cybersecurity management (CISO, etc.), and business unit leaders should actively participate in cyber	Customers shall conduct regular exercises and training to verify the effectiveness of the organization's cybersecurity incident response plans and emergency plans, and revise such plans based on the issues identified during the drills. When conducting recovery training, customers shall validate the appropriateness of system and data recovery processes, as well as the rationality of the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). Customers shall implement a combination of various types of training and exercises, and may engage external contractors to participate in the drills when necessary. Customers may avail themselves of the Tencent Cloud Smart Advisor (TSA) service to support the planning and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		exercises and training and personally understand the results. ③ When developing exercise and training scenarios, include severe but plausible scenarios that could have a significant impact on customers. ④ Regularly validate the effectiveness of the cyber incident response plan and contingency plan from the perspective of business continuity through exercises and training, and revise the plans based on challenges, lessons learned, and other findings from the exercises and training. ⑤ Review the methods, scenarios, and other aspects of exercises and training in response to the latest threat trends and developments. [Desirable Response Measures] a. Include verification of the appropriateness of system and data recovery procedures, as well as the validity of recovery objectives, in recovery training using actual equipment or similar setups. b. Conduct exercises and training using scenarios that could cause widespread and long-lasting incidents affecting the organization itself, or incidents such as connection failures to exchanges, clearing and settlement institutions, etc., which could have severe ripple effects across the entire financial system. c. For improvements addressing issues identified through exercises	implementation of business continuity testing. As a cloud governance platform for vertical applications across multiple IT Operations Management (ITOM) domains, TSA leverages the extensive experience of Tencent Cloud's massive team of O&M experts to optimize cloud infrastructure through multiple governance measures such as risk inspections and fault drills. TSA provides a full range of fault injection scenarios covering Infrastructure as a Service (IaaS) to Platform as a Service (PaaS), as well as drill experience templates for various industries, which cover multiple typical application scenarios such as cross-availability zone disaster recovery. It helps customers quickly and efficiently reuse mature solutions based on their own business needs, thereby improving system availability. To assist customers in complying with regulatory guidelines, 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 often conducted by simulating real and classic disaster recovery scenarios, including adversarial attack and defense and large-scale failures, to comprehensively verify the system's disaster recovery capability, response speed and recovery capability. After the drills, the relevant departments organize the compilation of drill reports, implement rectifications in accordance with the identified improvement measures, and file and retain the reports for record-keeping purposes. Tencent Cloud reviews and updates its

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and training, either conduct follow-up exercises to verify their effectiveness, or obtain approval from senior management, etc., for accepting the residual risk.	business continuity management system on an annual basis, and conducts reviews of the business continuity plans and disaster recovery plans for relevant products and services based on the results of business impact analysis, with updates made as needed.
		d. Implement combined exercises and training by integrating various types considering their respective scale and characteristics.	Where appropriate, Tencent Cloud may also provide relevant technical support for customers' security drills.

6.3 Defense Against Cyberattacks

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.3	Defense Against Cyberattacks	[Basic Response Measures] ① Implement a multi-layered defense approach by combining multiple levels of cybersecurity measures to prepare for cyberattacks, including perimeter network defenses to prevent unauthorized intrusions, internal network measures to prevent unauthorized system use, and measures to prevent information leakage to external parties.	Customers shall adopt multi-layered defense measures to guard against cyberattacks. To implement network perimeter protection, 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. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks, ensuring stable and secure business operations. In terms of network communication security, customers' communications on the Tencent Cloud Console are protected by encryption through the HTTPS security protocol. To enable customers to securely and quickly access cloud-based business systems from any location, at any time, and via any mainstream terminal, Tencent Cloud supports SSL VPN remote access technology. SSL VPN protects the security of data transmitted over the Internet through encryption, and also supports appropriate access control to reduce the occurrence of unauthorized access. In addition, Customers can also use Cloud Connect Network (CCN) to establish secure private interconnections between VPCs or between VPCs and on-premises data centers (IDCs). To assist customers in complying with regulatory guidelines, Tencent Cloud has established network security management specifications and a network defense-in-depth system. Tencent Cloud has defined network security control and protection standards as well as corresponding roles and responsibilities through management systems and processes, ensuring the secure operation of businesses hosted on Tencent Cloud's network. Meanwhile, Tencent Cloud designs its network security architecture with reference to industry best practices, divides security domains based on business functions and security risks, implements physical or logical isolation for different security domains, and ensures the security of office networks and production networks

No.	Domain	Summary of Controls	Tencent Cloud's Response
			through access control, boundary protection and other measures. Tencent Cloud adopts multiple protection mechanisms such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, and web security protection to detect, filter and block malicious network traffic in a timely manner, thereby protecting Tencent Cloud's network security. For multi-tenant data isolation, Tencent Cloud strictly adheres to the principle of data confidentiality and adopts multi-layered technical isolation measures. Through such security mechanisms as resource access control policies at the virtualization control layer, isolation policies between private networks within the cloud platform, permission assignment and identity authentication on the Web Console, as well as interface session IDs and access keys, Tencent Cloud ensures that no tenant can access, obtain or tamper with the data of other tenants. In terms of data loss prevention, Tencent Cloud implements end-to-end identity verification and maintenance for data access permissions to safeguard the integrity of data assets and the reliability of business services, and has established a real-time monitoring and interception mechanism to detect and block any abnormal data access behaviors. In addition, Tencent Cloud has deployed Data Loss Prevention (DLP) tools on employees' office terminals to effectively restrict data export and monitor, detect and prevent potential data theft activities.
2.3.1	Authentication and Access Management	[Basic Response Measures] ① Establish policies, regulations, etc., regarding authentication and	Customers shall formulate norms and procedures for authentication and access permission granting, and conduct regular permission reviews. They shall properly

No.	Domain	Summary of Controls	Tencent Cloud's Response
		access rights assignment, and review them regularly.	safeguard the identity authentication information of devices and users, take measures to identify users and verify their access permissions before they access the system, and record user operations and processed content in logs. In addition, customers shall manage, protect and document physical access to highly confidential areas and critical premises such as computer rooms and data storage rooms.
		② Grant system access rights only to individuals who have a legitimate business need, have received proper authorization, and have undergone appropriate education/training and are under management. Additionally, grant users' access rights to devices and systems considering the importance of the system and information.	In terms of access control management, <u>Cloud Access Management (CAM)</u> enables customers to securely and granularly manage access to Tencent Cloud products and resources. The root user account holds full access permissions to the resources under its name by default, and can create sub-users and assign identity IDs, credentials, and permissions to them. CAM supports multi-factor authentication through various methods, including verification via MFA devices or mobile verification codes, so as to verify the security and reliability of the user identity and environment prior to login and sensitive operations. CAM also supports the use of <u>CloudAudit</u> to conduct supervision, compliance checks, operation audits, and risk audits on Tencent Cloud account activities.
		③ Appropriately manage device and user IDs and authentication information.	
		④ Verify the appropriateness of a user's access rights before authenticating the ID and granting access to the system. Also, implement measures to identify the accessing user, log processing details, and link them to the user's operations.	
		⑤ Determine authentication requirements based on the importance of the system and information. In particular, use multi-factor authentication for remote access to critical systems.	
		⑥ Utilize mechanisms and initiatives to prevent fraudulent activities by third parties, secure file exchange functions, customer support and awareness activities.	Tencent Cloud also provides <u>Bastion Host (BH)</u> , which supports fine-grained authorization based on dimensions such as users, assets, accounts, and operation permissions, ensuring that the permissions held by users are the minimum required for them to access assets and complete work tasks. Bastion Host also features operation audit functionality, which records and analyzes user operation logs to enable effective traceability of security incidents.
		⑦ Ensure confidentiality, integrity, and authenticity in authentication and authorization across systems or security boundaries, such as with single	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		sign-on (SSO) or external authentication federation.	To assist customers in complying with regulatory guidelines, Tencent Cloud has formulated internal access control management norms, requiring user accounts to use unique identifiers and setting password policies for employee accounts in accordance with security baselines. Tencent Cloud implements admission authentication for employees through a zero-trust security management system, and users must complete two-factor authentication before accessing internal resources.
		⑧ Manage, protect, and record physical access to high-security areas and important rooms such as computer rooms and data storage rooms.	
			Tencent Cloud has also established internal authorization policies and a segregation of duties matrix mechanism. Permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights. It maintains records of the identity information of personnel corresponding to job roles and their permission levels across various business systems, and conducts regular internal permission reviews to prevent the abuse and misuse of permissions. In addition, jump servers have been fully deployed in Tencent Cloud's production environment, which centrally manage the administrator account permissions for back-end system components. Access to jump servers requires authorized approval and is restricted to specific internal O&M personnel of Tencent Cloud, with appropriate identity authentication required for login. All O&M operation records are centrally stored on a log platform and regularly audited by Tencent Cloud's internal audit team.
			In terms of physical access control, each Tencent Cloud data center has formulated strict access control policies in accordance

No.	Domain	Summary of Controls	Tencent Cloud's Response
			with regional security requirements of different levels. All visitors and staff must undergo identity verification and personal item checks, and register their carried items when entering or exiting the data center. Based on personnel categories and access permissions, Tencent Cloud has established a complete physical access control security matrix in the data center's access control authorization system, achieving effective management and control over the access and operation behaviors of all personnel in the data center. Furthermore, the physical computer rooms in Tencent Cloud's financial special zones adopt dedicated enclosures to physically isolate the equipment of different customers, and are equipped with biometric access control systems, which can effectively prevent unauthorized personnel from accessing customers' equipment.
2.3.2	Education and Training	[Basic Response Measures] ① Regularly provide cybersecurity awareness education and training tailored to their roles and responsibilities for all employees and executives, including senior management. ② Ensure that personnel from third parties receive the necessary cybersecurity education and training to properly perform their duties. Note: This requirement includes the financial institution verifying that the third party has conducted internal education and training. ③ Implement necessary initiatives to raise customer awareness about cyber threats and cybersecurity as needed.	Customers shall provide all employees with necessary education and training on a regular basis to maintain and enhance the professional skills and knowledge of relevant employees, and ensure that the on-duty responsible personnel of third parties have received the cybersecurity education and training essential for performing their duties. In addition, customers shall, as needed, take measures for their own organizational customers to help them understand cyberattack threats and raise their cybersecurity awareness. The operation procedures, user manuals and other documentation for Tencent Cloud products have been formalized and are available to customers via the official website. Tencent Cloud also provides customers with Tencent Cloud training and certification programs based on Tencent Cloud product knowledge and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		④ Regularly provide education and training for employees and executives in IT or security departments to maintain up-to-date knowledge and skills regarding evolving threats and countermeasures. ⑤ Ensure that all employees and executives have access to necessary education and training opportunities to respond appropriately if they become involved in an incident. Additionally, regularly provide education and training on roles and operational procedures within the incident response and recovery plan to relevant personnel. [Desirable Response Measures] a. If forensic investigations, etc., are conducted internally by employees, maintain and enhance the relevant employees' skills and knowledge. b. If vulnerability assessments or penetration testing are conducted internally by employees, maintain and enhance the relevant employees' skills and knowledge.	relevant professional capabilities, so as to enhance customers' technical proficiency and cloud service competency. To assist customers in complying with regulatory guidelines, Tencent Cloud has established a training mechanism that requires regular employees, consultants, interns and outsourced employees to complete training courses. Tencent Cloud offers a diverse range of training courses, including mandatory training for all staff, special training for key positions and optional professional courses, covering basic security awareness, office security, vulnerability identification and defense, privacy protection, emergency response, R&D security specifications and data security requirements.
2.3.3	Data Protection	[Basic Response Measures] ① Establish a data management policy based on the importance of the information and the specific risks inherent in the technology environment where it is used. This policy should include data management, data storage, adoption of appropriate encryption methods, lifecycle management and protection of encryption keys	Customers shall formulate and implement data management policies, management procedures for the protection and use of external storage media, and backup procedures to protect and manage data throughout its lifecycle. Customers shall introduce a Data Loss Prevention (DLP) system or an equivalent solution to monitor and prevent data leakage caused by employees or external relevant personnel. In terms of data storage protection, Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and digital certificates, and response procedures in case of compromise. ② Classify data according to its level of importance and protect it in accordance with the management policy corresponding to each classification. ③ Establish and implement management procedures for the protection and use of external storage media. ④ Appropriately manage data throughout its entire lifecycle. ⑤ Establish and implement regulations, etc., regarding backup, including backup requirements based on the importance of systems and information, isolation and protection of backup data, integrity verification, and execution of recovery tests. For clearing and settlement institutions, etc., establish agreements with relevant parties regarding data sharing as necessary to ensure the integrity of backup data. [Desirable Response Measures] a. Implement Data Loss Prevention (DLP) or equivalent solutions to monitor and protect against data leakage by employees or external parties. b. Establish data governance policies, regulations, etc., based on legal responsibilities and the importance of information as an organizational asset.	Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption 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. Invalid, expired, or compromised keys are securely deleted using reliable methods, and once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. In addition, Tencent Cloud adopts multi-copy redundant storage and erasure coding technology for data storage, and immediately takes necessary recovery measures upon detection of integrity errors, which greatly enhances 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. In addition, Customers can also 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)

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • <u>Cloud Connect Network (CCN):</u> CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal path selection, and fast failover capabilities. All communication within CCN remains off the public internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further enhances communication reliability, making data transmission secure and dependable. In terms of backup management, Tencent Cloud provides customers with multi-storage replica and backup services based on the functions of its cloud products and services and assumes liability for the provided data backup services in accordance with the provisions stipulated in the product service level agreements. Various Tencent Cloud products and services including computing services, network services, storage services, database services, container and middleware services enable customers to configure backup strategies for their own systems and data, meeting their diverse backup needs. For more information related to backup, please refer to the content in Clause 39 Data File Management of Section 5.2.3 in this Guide.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			In terms of data loss prevention, Tencent Cloud provides customers with the Data Security Audit (CDS) service. As an artificial intelligence-based database security audit system, CDS supports full audit and storage of all types of database session information, access operations and SQL statements within an enterprise's network. It identifies malicious acts in operations based on multiple rule bases and threat detection engines, and promptly notifies administrators to take corresponding security protection measures. For data deletion and destruction, Tencent Cloud provides a secure and reliable data destruction mechanism. Upon the termination of a customer's services, Tencent Cloud will adopt stringent data erasure methods completely delete all customer data (including replicas and backups) upon the expiration of the retention period; the deleted data shall be irrecoverable. 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 scrapped, Tencent Cloud will promptly conduct complete physical destruction in accordance with rigorous processes. To assist customers in complying with regulatory guidelines, Tencent Cloud has established relevant management procedures for data security, which clarify the principles of data classification and grading as well as data protection. The procedures require data owners to implement corresponding security protection measures throughout the entire data lifecycle – including data collection, transmission, access control, backup,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			transaction protection, and the management of information transmission with third parties – in accordance with the requirements of data classification and grading, so as to safeguard the confidentiality, integrity and availability of data. Customer data is classified as data of a high security level within Tencent Cloud, and customers hold exclusive ownership and control over the content of their own data. Unless it is necessary for service provision or troubleshooting, and with the explicit authorization of customers, or in cases compliant with national laws and regulations such as investigations into criminal incidents by national or local government authorities, no internal employee of Tencent Cloud will proactively access any customer data. In addition, Tencent Cloud implements end-to-end identity verification and maintenance for data access permissions to safeguard the integrity of data assets and the reliability of business services, and has established a real-time monitoring and interception mechanism to detect and block any abnormal data access behaviors. Tencent Cloud has also deployed DLP tools that can restrict the external export of data on employees' office terminals to monitor, detect and prevent potential data theft activities.
2.3.4	System Security Measures	2.3.4.1. Hardware and Software Management [Basic Response Measures] ① Configure systems to provide only necessary functions. ② Establish procedures to ensure cybersecurity during system maintenance.	Customers shall configure systems to provide only necessary functions, formulate relevant procedures to ensure cybersecurity during system operation and maintenance, and protect systems from malware infection. For hardware and software reaching end-of-support, customers shall establish plans for their secure decommissioning or upgrade. In addition, customers shall set security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		③ Plan and securely implement the retirement or replacement of hardware and software upon end of support. If updating software to a supported version is difficult, implement complementary measures and establish and steadily execute a migration plan to systems and business processes using software for which support can be obtained promptly. ④ Protect systems from malware infection. [Desirable Response Measures] a. For third-party libraries, middleware, and hardware used in systems, select secure products from vendors who incorporate secure development practices such as Security by Design and Security by Default into their product development, to avoid backdoors or other unauthorized access points. b. Include cybersecurity risks related to hardware in supply chain risk assessments. c. Ensure the authenticity of hardware (devices, firmware, UEFI, or BIOS, etc.) and implement measures to prevent unauthorized modification. d. Establish secure procurement standards within hardware procurement criteria. Require suppliers or trading partners to comply with laws, organizational security standards, or ethical standards in procurement or trading agreements. Create and	procurement standards for hardware purchases and incorporate considerations of hardware-related cybersecurity risks into supply chain risk assessments. Customers may adopt the Cloud Workload Protection Platform (CWPP). Leveraging Tencent's massive accumulated threat data, this service helps customers manage baseline security. CWPP supports baseline detection with optional modes such as one-click detection and scheduled detection, and allows viewing of baseline compliance rates and remediation recommendations. It also provides Tencent Cloud's default baseline policies to facilitate customers' better management of server baseline security. The Cloud Security Center (CSC) offers automated inspection and assessment capabilities for cloud product configuration risks, covering a variety of cloud products including Cloud Virtual Machines, Object Storage, Cloud Databases and Load Balancers. This helps customers mitigate security risks arising from incorrect security configurations in cloud product usage and elevate the overall cloud security posture. Meanwhile, customers can achieve centralized audit and governance of cloud resources through Config Audit. It continuously records the configuration information and configuration changes of various cloud resources across different regions under customer accounts, and automatically conducts ongoing compliance assessments of cloud resource configurations under enterprise accounts based on Tencent Cloud best practice rules and compliance package templates to identify non-compliant resource configurations, thus enabling automated monitoring and management of cloud resources.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		maintain supplier lists or sanctions lists based on laws, internal standards, and UN sanctions, and conduct procurement accordingly.	To assist customers in complying with regulatory guidelines, Tencent Cloud maintains a detailed inventory of hardware and facilities through a Configuration Management Database (CMDB), which includes the End-of-Support Date and version information for each server. Tencent Cloud regularly decommissions and replaces servers, and upgrades software components (such as operating systems and database systems) to appropriate versions before their end-of-support date. For decommissioned hard drives, Tencent Cloud adopts secure physical destruction methods to ensure complete destruction, with all destruction activities recorded in formal documentation. In terms of host security, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to conduct comprehensive monitoring and management of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance audits for command operations and login behaviors, and trigger alerts upon detection of malicious programs and abnormal activities. In terms of secure development, Tencent Cloud has established a set of information system secure development standards, striving to integrate the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System and ISO/IEC 9001 Quality Management System Standard into the entire product secure development lifecycle, covering key stages such as requirements, design, development, testing,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			delivery and operation and maintenance. Tencent Cloud adopts an agile development approach, integrated with essential Software Development Lifecycle (SDLC) principles and Security-by-Design principles, to ensure that cloud products receive robust security controls throughout their lifecycle. In terms of baseline and configuration management, Tencent Cloud has established a set of cybersecurity configuration standards and security baseline standards, aiming to standardize the security configuration management of network devices, firewalls, host server operating systems, databases and application systems. Tencent Cloud uses scanning tools to scan the configurations of operating systems, database management systems, network devices and virtual images, continuously detecting deviations from the standard configurations defined in baseline documents. Once deviations from the standards are identified, the system automatically generates security tickets and sends them to the responsible departments for timely handling. For more information related to hardware and software security, please refer to the content in Section 5.2.4 Management of Various Devices of this Guide.
		2.3.4.2. Log Management [Basic Response Measures] ① Establish procedures for log collection, monitoring, and retention, and review them regularly. ② Regularly or as needed, verify the appropriateness of event logs from information systems and	Customers shall formulate procedures for the collection, monitoring and retention of logs and conduct regular reviews of such procedures. They shall also review information system event logs and the operation logs of O&M personnel on a regular or as-needed basis. Tencent Cloud provides customers with Cloud Log Service (CLS). As an all-in-one log service platform, CLS offers a full range

No.	Domain	Summary of Controls	Tencent Cloud's Response
		operation staff work logs.	of services including log collection, storage, search and analysis, real-time consumption, and log delivery, assisting customers in addressing issues related to business operation, security monitoring, log auditing and log analysis. CLS adopts a highly available distributed architecture design and stores log data with multi-redundant backups to prevent data unavailability caused by single-node service downtime, achieving high service availability and providing stable and reliable service guarantees for log data. The Cloud Security Center (CSC) also supports the collection of various cloud security-related data such as alert data from cloud security products, cloud asset configuration change data, operation behavior data of cloud users, and log data from some cloud products, and provides a unified search and investigation platform to help customers achieve comprehensive cloud log auditing, search and investigation. In addition, the Elasticsearch Service (ES) aggregates and transmits real-time logs from other cloud products such as Cloud Virtual Machines and containers, as well as historical and incremental business data of services, to Tencent Cloud ES clusters for distributed data storage, query and analysis. For the collection and retention of operation logs, customers may adopt CloudAudit to monitor Tencent Cloud account activities and conduct compliance checks, operation reviews and risk audits. CloudAudit supports online viewing of operation records of the Tencent Cloud Console and cloud APIs from the past 90 days, including information such as access keys, regions, error codes, event IDs, event names, event sources, event time, request IDs, source IP

No.	Domain	Summary of Controls	Tencent Cloud's Response
			addresses and usernames.
			Tencent Cloud has also established internal norms and mechanisms for log collection and management to control the recording, extraction, storage, protection, analysis and auditing of login logs, operation logs, regular system logs, system security event logs and other log types, so as to detect and prevent abnormal system activities and risks. Logs are centrally aggregated into Tencent Cloud's log management platform for unified management, and relevant log information is subject to backup and stringent protection measures to prevent unauthorized modification and deletion. Backup logs are retained for more than one year. Tencent Cloud conducts log audits through automated O&M security audit tools and its internal audit team to detect system or operational anomalies and mitigate operational risks.
		2.3.4.3. Security by Design [Basic Response Measures] ① Practice "Security by Design" by incorporating security requirements from the planning and design stages of financial products and services. Verify risks and implement countermeasures across the entire service flow, including important third parties. ② Confirm that critical third parties providing systems to your organization have the necessary framework in place to implement Security by Design. [Desirable Response Measures] a. Establish and operate a management process for Security by Design.	Customers shall implement Security-by-Design in the design phase of financial products and services, and ensure that key third parties providing systems to the organization have mechanisms in place to implement Security-by-Design. Customers shall also establish and operate management processes relevant to Security-by-Design. To support customers in R&D lifecycle management, Tencent Cloud provides Cloud-Native Build (CNB) as a developer tool. Based on the Docker ecosystem, CNB abstracts environments, caches and plugins and adopts a declarative syntax, aiming to help developers build software in a more efficient manner. It offers a complete developer toolchain with capabilities including code hosting, high-performance R&D pipelines, AI code review, cloud-based development environments, artifact

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management and custom task sets, which effectively enables full-lifecycle R&D support from requirement analysis to deployment and facilitates agile development management. 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 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Release: Systems are deployed to production only after all high-risk issues have been fixed. In addition, Tencent Cloud strictly segregates development environments from production environments through physical and logical isolation mechanisms, and prohibits the use of non-anonymized production data in non-production environments.
		2.3.4.4. Technical Measures for Infrastructure (Network, etc.) [Basic Response Measures] ① To prevent unauthorized intrusion, implement appropriate intrusion prevention measures at connection points between external networks and internal networks. Also, implement intrusion prevention measures for data exchange between external and internal networks. ② Regularly and upon system environment updates, inspect and update network device configurations (firewall rules, ports, protocols, etc.). Configure firewalls to allow only necessary communications. ③ Ensure network security through dedicated lines, encryption technologies, etc., from the perspective of protecting data confidentiality and integrity. ④ Implement appropriate authentication and access control functions for wireless LAN network access to prevent unauthorized use. ⑤ Limit and properly manage	Customers shall implement intrusion prevention measures for data exchange between internal and external networks, and ensure network security through dedicated lines, encryption technologies and other means. They shall refine network segmentation, and enhance the resilience of the organization's communication and network services through countermeasures against DDoS/DoS attacks, DNS-related cybersecurity measures, alternate communication path control and other initiatives. In addition, customers shall restrict and manage systems requiring remote access such as those for remote work or supplier maintenance. In terms of network communication security, all customer communications on the Tencent Cloud Console are protected by encryption via the HTTPS security protocol. The cloud API interfaces provided by Tencent Cloud's cloud products feature security capabilities including HTTPS encryption, signature verification and status monitoring, delivering port-level communication security for customers' businesses. Customers can also further enhance data transmission security using the following services: <u>Direct Connect (DC)</u>: Provides dedicated, high-security, high-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		systems subject to remote access for telework or vendor maintenance. For critical systems, use multi-factor authentication and encrypted connections. [Desirable Response Measures] a. Enhance the resilience of organizational communications and network services through measures such as DDoS/DoS attack protection, cybersecurity measures for DNS, and control of alternative communication routes. b. Separate development and test environments from production environments and prevent unauthorized access and unauthorized modification of information assets. c. Segment networks finely to prevent the spread of cyberattacks, such as by blocking malware lateral movement.	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. To safeguard network resilience, Tencent Cloud data centers are deployed across multiple regions worldwide, with the network egress of each Availability Zone connected to multiple ISPs. This builds the cross-regional disaster recovery capability of the Tencent Cloud network, effectively mitigating the sustained impact of public network failures caused by ISPs. The Tencent Cloud underlying network adopts a redundancy architecture, and in conjunction with traffic engineering scheduling for route-level path priority and reachability, ensures that network services are not interrupted by single-point device failures. Tencent Cloud also offers a range of services to help customers effectively manage network security: • <u>Virtual Private Cloud (VPC)</u>: Based on tunnel technology, it constructs virtual networks over physical networks and leverages virtualization technology to achieve complete logical isolation between different VPCs, providing customers with independent and isolated secure cloud networks. For CVM instances within a VPC, traffic control at the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			instance and subnet levels for inbound and outbound traffic is implemented by configuring security group and network ACL rules, enabling network access control at different layers. • <u>EdgeOne (EO)</u>: It provides customers with security protection and acceleration services based on Tencent's global edge nodes, featuring capabilities such as DDoS protection, intelligent web protection, BOT/crawler attack protection and DNS resolution, and supports customers in configuring custom access control rules based on business needs. Customers may also opt for network perimeter protection tools including Cloud Firewall, Web Application Firewall and Anti-DDoS. • <u>Cloud Firewall (CFW)</u>: It supports active firewall ACL management, real-time IPS interception, virtual patching and malicious code detection, providing customers with protection for different network perimeters. • <u>Web Application Firewall (WAF)</u>: It helps defend against website and web business security threats such as web attacks, intrusions, vulnerability exploitation, malicious code injection, page tampering, backdoor attacks and crawling. • <u>Anti-DDoS</u>: It addresses DDoS attacks with abundant and high-quality DDoS protection resources combined with continuously evolving proprietary and AI-driven detection algorithms.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• Flow Logs (FL): It supports real-time, non-intrusive out-of-band collection, storage and analysis of network traffic, helping customers resolve issues such as troubleshooting, architecture optimization, security detection and compliance auditing. To assist customers in complying with regulatory guidelines, Tencent Cloud has established network security management norms and a network defense-in-depth system. Through management systems and processes, Tencent Cloud defines clear network security control and protection standards, as well as corresponding roles and responsibilities, ensuring the secure operation of businesses hosted on the Tencent Cloud network. Meanwhile, Tencent Cloud designs its network security architecture with reference to industry best practices, divides security domains based on business functions and security risks, implements physical or logical isolation for different security domains, and safeguards the security of office and production networks through access control, perimeter protection and other measures. Tencent Cloud leverages multiple protection mechanisms including firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection and web security protection to detect, filter and block malicious network traffic in a timely manner and protect the security of the Tencent Cloud network. In terms of firewall usage and management, Tencent Cloud's firewall rules are configured to restrict access to its production network. Administrative access to firewall rules is limited to authorized

No.	Domain	Summary of Controls	Tencent Cloud's Response
			personnel using the Secure Shell (SSH) protocol and two-factor authentication, and all changes to firewall rules undergo relevant review and approval processes before deployment. Tencent Cloud conducts comprehensive regular audits of firewall rules, with a focus on verifying rule usage. In terms of network device security, Tencent Cloud has established a set of network security configuration standards and security baseline standards to standardize the management of security configurations for network devices, firewalls, host server operating systems, databases and application systems. Tencent Cloud regularly reviews the security policies and parameter settings of network devices such as routers, firewalls and network servers to ensure their effectiveness. Tencent Cloud has also deployed an internal network monitoring system to monitor network devices and trigger alerts, and follows up on and resolves identified security issues through a ticketing system. In terms of remote access management, Tencent Cloud has established internal procedures for the management of employee remote access. Employees may only use trusted devices registered on Tencent Cloud to remotely access the Tencent Cloud office network and daily office systems via encrypted communication channels. Tencent Cloud maintains remote access logs to record user operation behaviors. Meanwhile, Tencent Cloud's internal office network is completely isolated from the production environment where customer data is stored. When Tencent Cloud employees obtain customer consent and authorization to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			access customer information assets, they must access the production environment of customer data through jump servers. All back-end O&M operation records are centrally stored on a log platform and regularly audited by Tencent Cloud's internal audit team.
	2.3.4.5. Measures for Cloud Service Usage	Customers shall understand the specifications and the shared responsibility model of the cloud services they use, and verify the impacts of any changes to service specifications in accordance with the division of responsibilities. They shall ensure the appropriateness of all configurations and settings for cloud services, establish information sharing and incident response mechanisms with relevant stakeholders, and confirm the handling method of data stored on cloud services when terminating the use of such services.	
	[Basic Response Measures]		
	① Confirm and deepen understanding of the specifications of the cloud services being used.		
	② Understand the shared responsibility model and clearly define the scope of responsibilities between the organization and the cloud service provider.		
	③ Verify that there are no configuration errors in settings such as information disclosure. For validation, consider using expert system audits or diagnostic services for automatic misconfiguration detection as needed.		
	④ When service specifications change, confirm the impact according to the responsibility boundary.		
	⑤ Identify the various stakeholders involved and establish information sharing and incident response frameworks.		
	⑥ Confirm the handling of data on cloud services (logical disposal) when terminating cloud service usage.		

No.	Domain	Summary of Controls	Tencent Cloud's Response
			provider, Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Recognizing that customers' level of control varies depending on the type of cloud service selected (such as IaaS, PaaS, and SaaS), Tencent Cloud has established a Shared Responsibility Model for Cloud Security based on different service categories. For details, please refer to Section 3: "Tencent Cloud Security Responsibility Sharing Model." To assist customers with configuration checks and risk management, The Cloud Security Center (CSC) offers automated inspection and assessment capabilities for cloud product configuration risks, covering a variety of cloud products including Cloud Virtual Machines, Object Storage, Cloud Databases and Load Balancers. This helps customers mitigate security risks arising from incorrect security configurations in cloud product usage and elevate the overall cloud security posture. Meanwhile, customers can achieve centralized audit and governance of cloud resources through Config Audit. It continuously records the configuration information and configuration changes of various cloud resources across different regions under customer accounts, and automatically conducts ongoing compliance assessments of cloud resource configurations under enterprise accounts based on Tencent Cloud best practice rules and compliance package templates to identify non-compliant resource configurations, thus enabling automated monitoring and management of cloud resources. For communication with cloud users, Tencent Cloud has established multiple communication channels to facilitate

No.	Domain	Summary of Controls	Tencent Cloud's Response
			interactions with external customers, including the Cloud Console, email, and dedicated hotlines. The Cloud Console offers a ticketing service, enabling customers to report faults, incidents, issues and complaints related to security, availability and confidentiality. Tencent Cloud's ticketing system assigns priorities to customer tickets through a tiered response mechanism; when the first-line technical team is unable to resolve an issue effectively, the system will automatically trigger an escalation process, with the relevant product or technical team intervening to provide collaborative support, ensuring timely responses and resolution of customer needs and feedback. Customers may also select applicable service plans to access exclusive support, including dedicated support groups, technical account managers, and value-added services. Regarding change notifications, Tencent Cloud will notify customers of any change requests for products, infrastructure and network configurations that may affect the external environment via announcements, email, the Cloud Console and/or other appropriate channels. For incident response and notifications, Tencent Cloud has formulated an information security incident communication and early warning management procedure, and established clear warning and notification mechanisms for significant security incidents and major business disruption scenarios, and promptly inform and alert affected internal personnel, customers, and other relevant parties. This ensures orderly, timely and efficient communication and coordination among all parties. For security incidents that may

No.	Domain	Summary of Controls	Tencent Cloud's Response
			impact customers, Tencent Cloud will, after internal review and based on the scope and severity of the incident, notify customers of the handling and analysis results through appropriate means and provide corresponding technical support to assist them in taking remedial measures to minimize losses. In relation to the termination and exit of cloud services, if customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate their cloud-based data and production environments at any time. Tencent Cloud supports customers in backing up and migrating data in universal standard formats; customers may adopt the same transmission methods and protocols used for cloud migration, or use network service products such as Direct Connect (DC) and VPN Connection to ensure the secure and reliable transfer of data during cloud exit. Upon the termination of a customer's cloud services, Tencent Cloud will adopt strict data erasure methods completely delete all customer data – including copies and backups – upon the expiration of the retention period, with the deleted data being irrecoverable.

6.4 Detection of Cyberattacks

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.4	Detection of Cyberattacks	2.4. [Basic Response Measures] ① Establish procedures for monitoring, analysis, and reporting to detect early signs of cyberattacks, such as anomalies and Indicators of Compromise (IoC), and review them as necessary. Considering the risk	Customers shall formulate procedures for the monitoring, analysis and reporting of early indicators of cyberattacks such as anomalies and Indicators of Compromise (IoC), and take necessary monitoring and analysis measures based on the threat level of cyberattacks. They shall include cloud services in the scope of monitoring,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		that cloud services used could become an entry point for cyberattacks, include cloud services within the monitoring scope according to the shared responsibility model.	formulate corresponding incident response plans and emergency recovery plans for different types of cyberattacks, and review such plans on a regular or as-needed basis.
		② Implement necessary monitoring, analysis, and other countermeasures according to the threats posed by cyberattacks to reduce associated risks.	Customers may use Cloud Log Service (CLS) , an all-in-one log service platform that offers a full range of capabilities including log collection, storage, search and analysis, real-time consumption, and log delivery, assisting customers in addressing issues related to business operation, security monitoring, log auditing and log analysis. CLS supports the configuration of alert policies for one or more log topics; these policies execute monitoring tasks periodically and send alert notifications when the results of query and analysis meet the trigger conditions, enabling customers to detect abnormal issues in a timely manner. Customers may also use the Cloud Security Center (CSC) , which leverages its Asset Center, Risk Center, Alert Center and advanced security management features to build a closed loop of security operations covering proactive threat detection, in-incident response and remediation, and post-incident forensics and analysis. CSC supports periodic detection of six major categories of risks: port risks, vulnerability risks, weak password risks, content risks, cloud resource configuration risks and service exposure risks, and continuously monitors enterprise security status. It also centrally ingests log data from Cloud Firewall, Web Application Firewall and Host Security, providing unified auditing, analysis, aggregation, visualization and tracking of alert logs. In addition, customers may use the Elasticsearch Service (ES) to aggregate and transmit real-time logs from other cloud products such as Cloud Virtual
		2.4.1. Monitoring	
		[Basic Response Measures]	
		To detect early signs of cyberattacks, implement continuous monitoring of the following:	
		① Hardware and software.	
		② Network.	
		③ Employee access to systems.	
		④ Monitor access to systems by external service providers (e.g., maintenance activities).	
		⑤ Analyze whether detected early signs of a cyberattack constitute an incident and promptly report findings to the appropriate responsible personnel.	
		⑥ Periodically verify the validity of alert criteria, thresholds, and similar parameters used to detect early signs of cyberattacks.	
		⑦ Monitor entry/exit and suspicious activities in data centers and server rooms.	
		[Desirable Response Measures]	
		a. Implement mechanisms using honeypot accounts or servers to	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		detect attacks at an early stage.	Machines and containers, as well as historical and incremental business data, to Tencent Cloud ES clusters for distributed data storage, query and analysis.
		b. Conduct continuous monitoring considering the nature of customer service offerings.	
		c. Utilize tools such as SIEM (Security Information and Event Management) to aggregate multiple monitoring sources, and analyze in real-time whether detected early signs constitute an incident, including correlation analysis of the information.	In terms of network traffic monitoring, customers can opt for Flow Logs (FL) to perform real-time, non-intrusive out-of-band collection, storage, and analysis of network traffic, addressing needs such as troubleshooting, architecture optimization, security detection, and compliance auditing. To assist customers in complying with regulatory requirements, Tencent Cloud has established internal specifications and mechanisms for log collection and management, which govern the recording, extraction, analysis and auditing of log data such as login logs, operation logs and event logs to detect and prevent abnormalities and risks in system activities. Tencent Cloud has deployed an internal network monitoring system to monitor and trigger alerts for network devices such as routers, firewalls and network servers, and follows up on and resolves identified security issues through its ticketing system. Meanwhile, Tencent Cloud has defined detailed operational security red lines, and built a comprehensive rule base based on years of accumulated experience in abnormal behavior monitoring, as well as a robust automated operational security audit tool, which can promptly identify abnormal behaviors and automatically trigger real-time alerts. In terms of patch management, Tencent Cloud identifies the latest patches and conducts comprehensive security testing on them prior to installation to ensure patch security. Tencent Cloud regularly notifies all internal business teams to perform patch

No.	Domain	Summary of Controls	Tencent Cloud's Response
			upgrades and installations, and uses endpoint detection tools to scan the patch installation status periodically. An alert ticket is automatically generated for any device with overdue patch installations. In terms of physical security and monitoring, Tencent Cloud requires data center operators to equip data centers with 7×24-hour blind-spot-free video surveillance and alert systems, which are monitored by on-duty staff in the security room, and to ensure the secure retention of surveillance records for a sufficient period. Tencent Cloud also requires operators to arrange security personnel to conduct patrol inspections of all computer rooms and equipment in strict accordance with inspection checklists and schedules, who shall sign and record the inspection time at each check point. In the event of infrastructure failures or security incidents, the operators must immediately activate the emergency response procedures for the data center.

6.5 Response and Recovery from Cyber Incidents

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.5.1	Development of Incident Response Plan and Contingency Plan	[Basic Response Measures] ① Develop incident response plans and contingency plans (including recovery plans) for cyberattacks, categorized by type of cyberattack. Within these plans, define response priorities, target recovery time, and target recovery level. [Desirable Response Measures] a. Develop contingency plans to address large-scale cyber incidents, including incidents	Customers shall formulate corresponding incident response plans and emergency recovery plans for different types of cyberattacks, define response priorities as well as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and review such plans on a regular or as-needed basis. The emergency response plans formulated by customers shall include those for addressing large-scale cyber incidents. In terms of incident response and handling, Tencent Cloud has formulated

No.	Domain	Summary of Controls	Tencent Cloud's Response
		affecting financial settlement infrastructure or payment infrastructure, or incidents where services provided by third parties (including data centers or cloud services) are unavailable for extended periods.	internal information security incident management specifications, established an information security reporting, response and handling mechanism and related processes, and uses an internal security operation system to record security incidents. For detected and identified security incidents, Tencent Cloud will analyze and classify the incidents based on factors such as incident nature, data sensitivity level and impact scope, and promptly notify the relevant responsible personnel to follow up on the handling of the incidents. In terms of business continuity and emergency response planning, Tencent Cloud has built a comprehensive business continuity management system and obtained the international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud conducts Business Impact Analysis (BIA) on its cloud products and services to define the RTO and RPO for each business, and formulates differentiated response strategies and business continuity plans based on BIA results. Detailed disaster recovery plans have also been developed for cloud products and critical business 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 has also established a cybersecurity emergency response plan that covers a wide range of cybersecurity emergency scenarios such as cyberattacks, malicious programs, data security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			incidents, equipment and facility failures, and catastrophic events. Guided by the goals of improving and perfecting the emergency response plan system, building a dedicated emergency response team as the core support, and standardizing emergency response processes as the key focus, Tencent Cloud further enhances its capabilities in monitoring and early warning, incident notification and disposal, so as to prevent and mitigate the adverse impacts of cybersecurity incidents on its operations.
2.5.2	Response to and Recovery from Incidents	Incident response plans and contingency plans should consider the following: 2.5.2.1. Initial Response (Detection & Triage) [Basic Response Measures] ① Detect incidents through system monitoring (including items listed in Section 2.4), customer inquiries, or notifications from external organizations such as security response agencies. ② Based on information collected during detection/initial reception, verify facts and determine whether an incident response is required. ③ Prioritize incidents according to business impact, and report to the incident response team manager, the person responsible for overall cybersecurity management (e.g., CISO), and management, according to predefined criteria. 2.5.2.2. Analysis [Basic Response Measures]	Customers shall detect and verify security incidents through multiple channels to determine whether to activate incident response. For incidents requiring response, customers shall preserve evidence such as logs and maintain relevant records of all stages of incident response. In the event of an incident, customers shall promptly report it to regulatory authorities and other relevant parties in accordance with laws and regulations and the actual impact of the incident, and disclose appropriate information about the incident where necessary. Customers shall take containment measures to prevent the escalation of damages caused by cyberattacks and eliminate the root causes of such damages. They shall also conduct recovery in accordance with established recovery procedures, verify the status of systems and businesses after recovery, analyze and assess the causes of the incident post-recovery, and revise the relevant cybersecurity management mechanisms such as incident response plans and emergency plans as needed. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—

No.	Domain	Summary of Controls	Tencent Cloud's Response
		① For incidents deemed requiring a response, analyze the attack methods, root causes and pathways, impact on systems, current business impact, and potential future business impact. In particular, preserve evidence such as logs before analysis, and conduct the analysis using the preserved logs. ② Maintain records for each phase from incident detection/reception to recovery. 2.5.2.3. Customer Response, Internal/External Coordination, and Public Communications [Basic Response Measures] ① Ensure that responsible personnel and relevant parties from each contingency plan are familiar with their roles, necessary contact points, and required response procedures as defined in the incident response and contingency plans (including recovery plans). ② If customers are affected (e.g., by data leakage) and face secondary damage or other impacts, communicate the affected scope, precautions, and response methods to those customers. ③ When an incident occurs, promptly report to regulatory authorities, etc., in accordance with laws and regulations. ④ When disclosure is required by law or deemed appropriate from the perspective of preventing secondary damage or protecting	<u>Cloud Security Center (CSC)</u>. 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. To ensure that customers can quickly restore critical functions following a cybersecurity incident, a variety of Tencent Cloud products feature high availability to help customers achieve high availability of their systems or services, including the following: • <u>Cloud Load Balancer (CLB)</u>: It provides secure and efficient layer 4 and layer 7 traffic distribution services, expanding the external service capacity of application systems through traffic distribution and eliminating single points of failure. CLB is deployed in a cluster architecture and removes faulty instances in a timely manner to achieve high availability. • <u>Cloud Virtual Machine (CVM)</u>: It features high service availability and high data reliability. The Cloud Block Storage (CBS) attached to CVM adopts a triple-replica storage strategy, ensuring rapid data migration and recovery in the event of a failure of any replica. • <u>Tencent Kubernetes Engine (TKE)</u>: It adopts a distributed service architecture to enable automatic fault recovery and rapid migration of services; combined with distributed storage for the backends of stateful

No.	Domain	Summary of Controls	Tencent Cloud's Response
		customers, promptly and appropriately disclose known facts (e.g., damage from cyberattack, response status, recovery outlook) to customers and others, considering security risks to the organization and its stakeholders.	services, it achieves secure and highly available services and data.
		⑤ Share attack technique information (e.g., attacker TTPs - Tactics, Techniques, and Procedures) that could benefit other organizations, excluding confidential information, with information sharing organizations such as Financial ISAC or JPCERT/CC as needed.	To assist customers in collecting, aggregating and analyzing incident-related evidence, Tencent Cloud provides Cloud Log Service (CLS) . As an all-in-one log service platform, CLS offers a full range of capabilities including log collection, storage, search and analysis, real-time consumption, and log delivery, helping customers address issues related to business operation, security monitoring, log auditing and log analysis. In addition, the Elasticsearch Service (ES) aggregates and transmits real-time logs from other cloud products such as CVMs and containers, as well as historical and incremental business data, to Tencent Cloud ES clusters for distributed data storage, query and analysis.
	2.5.2.4. Containment	[Basic Response Measures]	
		① When taking containment actions to prevent the spread of damage from cyberattacks	For backup needs , a variety of Tencent Cloud storage and database services are equipped with backup functionalities to meet customers' diverse backup requirements. For customer data stored in the cloud, Tencent Cloud adopts real-time hot backup, redundant storage, remote backup and other methods to ensure the security, reliability and continuous availability of customers' business data in the cloud. Tencent Cloud also implements a number of protective measures such as physical security, access control and logical isolation, and supports customers in using the Key Management Service (KMS) and Cloud Access Management (CAM) to prevent unauthorized access to or tampering with their backup data. For more information on backups, please refer to the content in Clause 39 Data File Management of Section 5.2.3 of this Guide.
		[Desirable Response Measures]	
		a. During containment, appropriately notify third parties who may be affected by the response actions.	
	2.5.2.5. Eradication	[Basic Response Measures]	
		① Remove the root cause of the damage caused by the cyberattack (e.g., malware removal, patching to fix vulnerabilities).	
	2.5.2.6. Recovery	[Basic Response Measures]	
		① In the recovery plan, when determining recovery completion and business resumption, clearly define the decision-making	In terms of infrastructure recovery

No.	Domain	Summary of Controls	Tencent Cloud's Response
		authority and organize the decision-making factors. ② During recovery operations, perform actions such as initializing affected equipment and rebuilding systems to return the system to normal operation and confirm normal functioning. ③ When recovering from backups, be aware that backup data itself may have already been tampered with or infected with malware, depending on the attack method. ④ Before reconnecting affected systems to other systems, confirm that the system is operating normally and that the connection is properly established. ⑤ During recovery operations, confirm with system owners that critical business functions have been properly restored and are operating normally, verifying that the recovery has been performed appropriately. ⑥ After recovery from the incident, analyze the root causes of the incident and the factors contributing to the damage spread, and evaluate the response. Based on this evaluation, review and improve the cybersecurity management framework, including the incident response plan and contingency plan.	capabilities, Tencent Cloud data centers are deployed across multiple regions worldwide, with three data centers located in Hong Kong for customers to choose and deploy services in. The network egress of each Availability Zone is connected to multiple ISPs, building the cross-regional disaster recovery capability of the Tencent Cloud network and effectively mitigating the sustained impact of public network failures caused by ISPs. The power supply and air conditioning systems of all Tencent Cloud data centers adopt highly reliable fully redundant systems to avoid disruptions to the continuous power supply and cooling of data centers due to single points of failure. Tencent Cloud's underlying network and computing nodes are built with a redundancy architecture, ensuring the availability of network services and customers' businesses without interruptions caused by single points of failure. To assist customers in complying with regulatory requirements, Tencent Cloud has formulated information security incident management norms for incident response and remediation, established information security reporting, response and remediation mechanisms and relevant processes, and clearly defined the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud uses an internal security operation system to record security incidents. For detected and identified security incidents, Tencent Cloud will conduct analysis and classification based on factors such as incident nature, data sensitivity and scope of impact, and promptly notify the corresponding responsible persons to follow up on and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			handle the incidents. To assist customers in effectively fulfilling their communication and notification obligations, Tencent Cloud has established relevant procedures for information security incident response, incident escalation and incident notification to promptly issue early warnings or notifications to internal personnel, customers and other relevant parties who may be or have been affected by an incident, ensuring orderly, timely and efficient communication and coordination among all parties. For security incidents that may impact customers, Tencent Cloud will, after internal review and based on the scope and severity of the incident, notify customers of the handling and analysis results through appropriate means and provide corresponding technical support to assist them in taking remedial measures to minimize losses. In terms of incident management and evidence collection, Tencent Cloud has clearly defined internal standards for the collection of security incident evidence. During the process of security incident acceptance, investigation and assessment, handling, and follow-up, the relevant responsible departments maintain records of the accepted security incidents and ensure the integrity and confidentiality of such records. Based on an assessment of rationality and feasibility, Tencent Cloud provides effective support for customers' digital forensics and post-incident investigation and analysis of security incidents in accordance with their needs. Tencent Cloud has also established norms and mechanisms for log collection and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management to regulate the recording, extraction, storage, protection, analysis and auditing of various logs, including login logs, operation logs, regular system logs and system security incident logs. Logs are centrally aggregated and managed on Tencent Cloud's log management platform, with backup and stringent protection measures applied to all relevant log information. In terms of incident summary and continuous improvement, Tencent Cloud has put in place a periodic incident analysis mechanism. It conducts regular multi-dimensional analysis of incidents – covering incident type, occurrence frequency, scope of impact and severity – and adopts preventive measures based on incident reviews and root cause analysis to prevent the recurrence of similar incidents. For major security incidents, Tencent Cloud will set up a dedicated task force to compile a special analysis report and submit it to the senior management.

6.6 Third-Party Risk Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.6	Third-Party Risk Management	[Basic Response Measures] ① Consider the entire supply chain when formulating cybersecurity strategies and initiatives. Establish a cybersecurity management framework covering the entire business process, including third parties. ② Establish necessary structures and formulate a policy for third-party risk management to manage	Customers shall incorporate supply chain security into their cybersecurity strategies, plans and relevant mechanisms, establish a management system and organizational structure for third-party cybersecurity risk management, identify third parties and maintain a third-party management ledger, and formulate management processes for the termination of transactions with third parties. When conducting transactions with third parties, customers shall conduct due diligence in accordance with pre-defined criteria, and clearly specify the division of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		cybersecurity risks arising from third parties throughout the entire lifecycle of third-party relationships. ③ Establish an organizational structure for managing third-party risks and develop internal regulations. ④ Identify third parties and conduct risk assessments based on factors such as the positioning, role, and importance of the third party and the goods/services they provide within the organization's operations, whether they handle sensitive information, and their connectivity to internal systems. Implement risk-based responses accordingly. ⑤ Establish and maintain a register for managing third parties. ⑥ In incident response plans and contingency plans, establish arrangements that include third parties responsible for incident response. ⑦ Conduct due diligence based on predetermined criteria before initiating transactions with a third party. ⑧ Clearly define cybersecurity requirements for third parties and, based on importance, explicitly include the following items in contracts, SLAs (Service Level Agreements), or similar agreements with third parties. ⑨ Continuously monitor cybersecurity risks introduced by third parties and their	responsibilities between the two parties in the contracts or Service Level Agreements (SLAs) with third parties. Customers shall conduct risk assessments on third parties, and continuously monitor the cybersecurity risks posed by third parties and their products/services, the performance of contractual obligations, as well as the third parties' own supply chain risk management practices. For critical outsourced businesses, customers shall also formulate exit strategies or alternative plans. As a cloud service provider, Tencent Cloud offers online legal documents on its international portal 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, service terms and scenarios for agreement termination, dispute resolution mechanisms, notification mechanisms and other relevant provisions. Customers may also choose to sign offline agreements with Tencent Cloud to negotiate the terms and details of the agreements. For subcontracting scenarios, the aforementioned agreements include provisions on prior consent for subcontracting, notifications prior to the addition or replacement of subcontractors, data protection obligations and other relevant terms. Without the customer's prior consent, Tencent Cloud shall not subcontract any processing operations performed on behalf of the customer pursuant to the contract/agreement. Tencent Cloud shall notify customers via email and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		products/services, as well as contract compliance, according to the severity of the risks.	other channels of any intended changes involving the addition or replacement of subcontractors.
		⑩ Establish management processes for terminating relationships with third parties (e.g., data destruction, measures to block access to internal systems). [Desirable Response Measures] a. Assign personnel with appropriate knowledge and expertise to the centralized department responsible for third-party risk management. b. In third-party risk management, consider dependencies on third parties for critical operations, concentration risks of third parties, geopolitical risks, and the impact of fourth parties (i.e., third parties of the third party). c. Regularly monitor critical third parties' ability to manage their own third parties (including fourth parties, fifth parties, and Nth parties from the organization's perspective), their supply chain risks, and concentration risks. d. Develop appropriate contingency plans and exit strategies in advance to prepare for a critical third party's business withdrawal, operational halt, or contract termination, and regularly test alternative solutions.	In terms of subcontractor management, Tencent Cloud has established a comprehensive supply chain security management system, and effectively controls suppliers through stringent supplier security assessment and onboarding procedures, regular supervision and evaluation, and clear outsourced service agreements. This ensures that subcontracting will not affect Tencent Cloud's ability to provide relevant services to customers, the confidentiality and integrity of the customer information processing process, as well as the supervision and audit rights of financial institutions. To meet customers' requirements for the assessment, monitoring and management of outsourcing, Tencent Cloud shall provide relevant information upon customer request, and assign dedicated personnel to actively respond to and cooperate with customers' assessment, audit and investigation activities. In addition, Tencent Cloud undergoes professional audits by independent third parties on an annual basis, and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory authorities, company shareholders and other relevant stakeholders by providing attestation-level System and Organization Controls (SOC) reports. If customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate their cloud-based data and production environments at any time.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud supports customers in backing up and migrating data in universal standard formats; customers may adopt the same transmission methods and protocols used for cloud migration, or use network service products such as Direct Connect (DC) and VPN Connection to ensure the secure and reliable transfer of data during cloud exit. Upon the termination of a customer's cloud services, Tencent Cloud will adopt strict data erasure methods completely delete all customer data – including copies and backups – upon the expiration of the retention period, with the deleted data being irrecoverable. For more information related to outsourcing, please refer to the content in Section 5.1.2 External Controls of this Guide.

07

How Tencent Cloud Complies with the Payment Services Act

To ensure the proper provision of payment and settlement services, protect user security, facilitate the delivery of such services, and enhance the security and convenience of payment and settlement systems, the Financial Services Agency (FSA) of Japan has formulated and issued the Payment Services Act. This Act sets forth provisions and requirements primarily covering the issuance of prepaid payment instruments, fund transfer transactions conducted by non-deposit-taking institutions, electronic payment instrument transactions, cryptographic asset transactions, analysis of fund transfer transactions, and clearing of fund transfer transactions between deposit-taking institutions. The provisions of Article 21, Article 49, Article 62-10, and Article 63-8 of this act uniformly set information security management regulations for four types of payment-related service institutions, namely prepaid payment, fund transfer, electronic payment, and cryptocurrency transactions. These regulations require these institutions to take security management measures to prevent the leakage, loss, or damage of their business-related information, and ensure the security and controllability of the entire process of information processing.

As a cloud service provider, Tencent Cloud strictly complies with the laws and regulations of the jurisdictions where it operates its businesses, and is committed to providing customers with secure, stable, continuous and reliable cloud services. Tencent Cloud has assessed and improved its current control measures in accordance with the Payment Services Act.

In terms of information management and protection, customer data is classified as a high-security level of data within Tencent Cloud, and customers hold exclusive ownership and control over the content of their own data. To safeguard the security of customer information, Tencent Cloud has established relevant management procedures for data security, clarified the principles of data protection, and adopted a comprehensive set of protective measures including access control, physical infrastructure security protection, network protection, data encryption, data backup, and data loss prevention (DLP). Tencent Cloud also provides customers with a variety of cloud products and services to protect the confidentiality, integrity and availability of their data, such as storage and database products supporting data encryption and backup functions, as well as products related to communication and network protection. For more information about Tencent Cloud's information security measures and relevant cloud products/services, please refer to Chapters 5 and 6 of this Guide.

In addition, Tencent Cloud has obtained a number of security and privacy compliance certifications and qualifications through independent third-party audits and assessments, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF and SOC. These certifications attest that Tencent Cloud's security management and privacy protection frameworks meet the relevant certification standards and industry best practices. Specifically for the Japanese region, Tencent Cloud has assessed its current control measures in accordance with the FISC Security Guidelines for Information Systems of Financial Institutions, etc., and on this basis, compiled the corresponding System and Organization Controls (SOC) reports covering the control points related to the security, availability and confidentiality of the Tencent Cloud platform. For more information about Tencent Cloud's compliance status, please refer to [Section 2 of this Guide, Tencent Cloud Security and Privacy Compliance](#).

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 continuously providing secure, trusted, and intelligent cloud services to help enterprises efficiently embrace digital transformation and promote secure business growth.

This guide presents a comprehensive and transparent overview of how Tencent Cloud assists customers in achieving compliance for cloud-based systems and data based on the key regulatory requirements of the Financial Services Agency (FSA) and the Financial Services Information Systems Center (FISC) of Japan, helping enterprise customers host their systems and data on the cloud with confidence and peace of mind. Through this guide, Tencent Cloud aims to support enterprise customers in effectively meeting the compliance standards of regulatory authorities, while efficiently achieving digital transformation and innovative business development.

This user guide is for reference only. The customers should apply the information according to their actual circumstances to ensure regulatory compliance when using Tencent Cloud services.

09

Version History

Date	Version	Detail
April 2026	V1.0	Initial Release