



Tencent Cloud User Guide to Financial Industry Regulations & Guidelines in South Korea

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	7
2.2	ISO/IEC Certification	7
2.3	Regional and Industry Compliance.....	9
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 Electronic Financial Transaction Act	
06	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Regulation on Supervision of Electronic Financial Transactions	
6.1	Securing the Safety of Electronic Financial Transactions and Protecting Users.....	29
6.1.1	Personnel, Organization and Budget.....	29
6.1.2	Facility.....	31
6.1.3	Information Technology.....	35
6.1.4	Information Protection	48
6.1.5	Business Continuity.....	58
6.1.6	Vulnerability Analysis and Incident Response.....	65
6.2	Licensing, Registration, and Operations of Electronic Financial Affairs.....	70
6.3	Supervision of Electronic Financial Affairs.....	74
6.4	Standards for Evaluating the Soundness and Safety of Cloud Computing Service Providers	79
6.4.1	Information Protection and Law Observance	79
6.4.2	Personnel Security	82
6.4.3	Risk Assessment and Management	84
6.4.4	Service Supply Chain Management	86
6.4.5	Task Continuity Plan and Failure Recovery.....	87
6.4.6	Security Incident Response and Management	93
6.4.7	User Authentication and Access Control.....	97
6.4.8	Virtualization and Infrastructure Security.....	101
6.4.9	Development and Operation Security.....	108
6.4.10	Encryption and Data Protection.....	109
6.4.11	Physical Security.....	115
6.5	Continuity Plan for the Use of Cloud Computing Services.....	118
6.6	Safety Measures for the Use of Cloud Computing Services.....	129
6.7	Key Items to Be Included in the Cloud Computing Service Entrustment Agreement	146
07	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of	

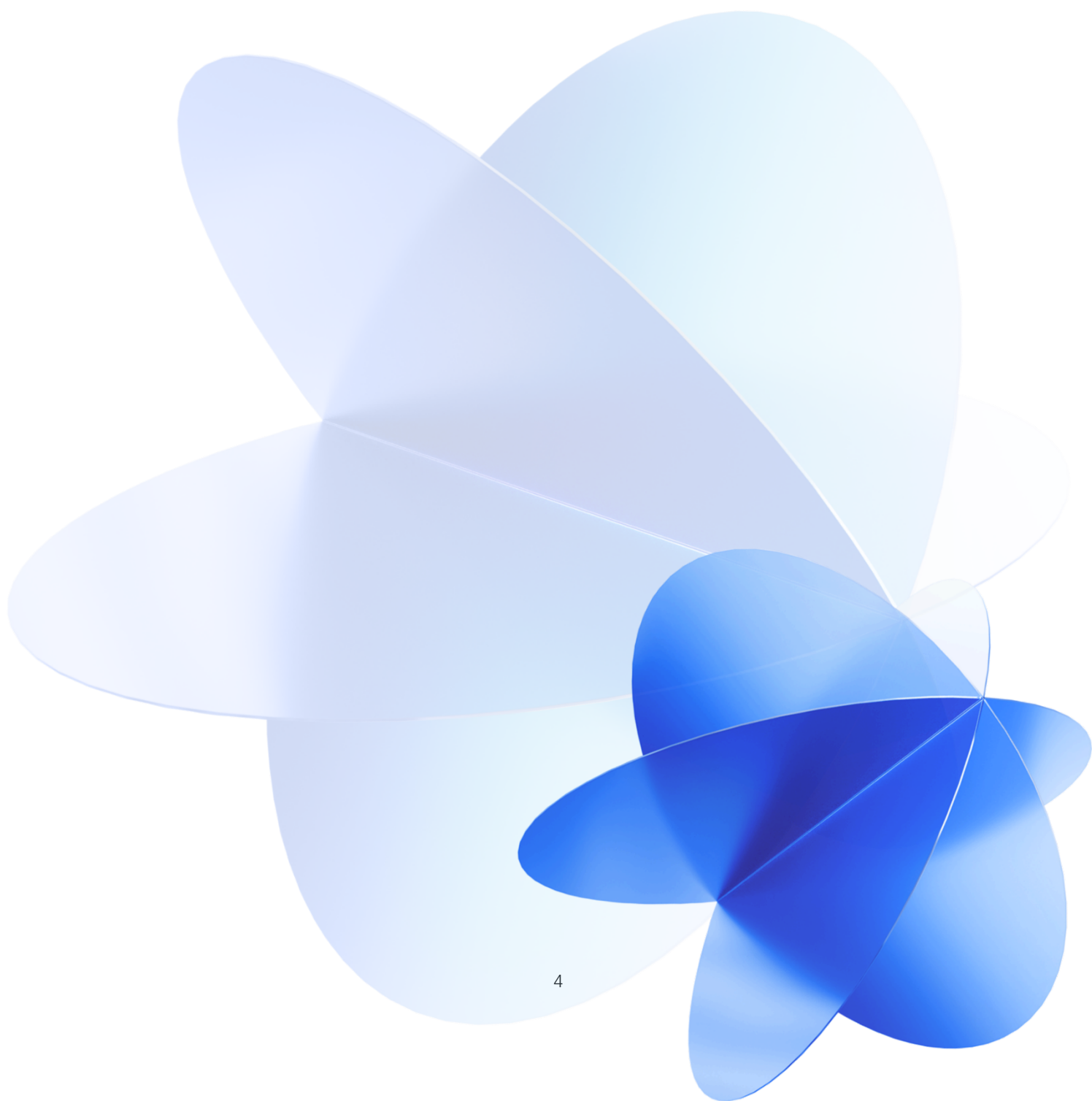
CONTENTS

Regulation on Entrustment, etc. of Duties by Financial Institutions

- 08 How Tencent Cloud Meets and Assists
Customers to Meet the Requirements of
Regulation on Outsourcing of Data Processing
of Financial Companies**
- 09 Conclusion**
- 10 Version History**

01

Overview



The Financial Services Commission (FSC) is a central government agency under the Prime Minister of South Korea. It has the statutory authority to draft and amend financial laws and regulations in South Korea and to issue regulatory licenses to financial companies. The FSC is committed to promoting the development of the financial industry, maintaining financial market stability, enforcing fair market practices, and protecting financial consumers. The Financial Supervisory Service (FSS) serves as the executive body of the FSC. Pursuant to directives issued by the FSC, the FSS is responsible for the implementation of financial policies, as well as conducting on-site inspections and off-site monitoring of financial companies.

Against the backdrop of accelerated digital transformation in the financial sector, financial companies in South Korea have a growing demand for new digital technologies such as cloud computing, big data, and artificial intelligence. To align with the needs of financial digitalization, address emerging risks and challenges, and safeguard the security and stability of South Korea's financial industry, the Financial Services Commission has issued a series of laws and regulations covering electronic financial transactions, outsourcing, information processing, and other areas. These regulations establish requirements and guidance for financial company¹, electronic financial service provider², and other entities to use cloud services in a secure and appropriate manner.

Tencent Cloud closely monitors the latest regulatory requirements issued by the Financial Services Commission of South Korea and is committed to assisting its financial institution customers in South Korea to meet relevant regulatory obligations. This document explains how Tencent Cloud supports customers in complying with regulatory requirements, with reference to the following four laws and regulations:

- [Electronic Financial Transactions Act](#)
- [Regulation on Supervision of Electronic Financial Transactions](#)
- [Regulation on Entrustment, etc. of Duties by Financial Institutions](#)
- [Regulation on Outsourcing of Data Processing of Financial Companies](#)

¹ "Financial Company" refers to an institution, organization, or business operator that falls under any of the following subparagraphs:

1) Institutions specified in Subparagraphs 1 to 5, 7, and 8 of Article 38, Paragraph 1 of the 「Act on the Establishment of the Financial Services Commission, etc.」 ;

2) Specialized Credit Finance Companies under the 「Act on Specialized Credit Finance Business」 ;

3) Postal institutions under the 「Act on Postal Savings and Insurance」 ;

4) Saemaul Geumgo (Village Credit Unions) and the National Federation of Saemaul Geumgo under the 「Saemaul Geumgo Act」 ;

5) Other institutions, organizations, or business operators engaged in financial business and finance-related operations in accordance with legal provisions, as designated by Presidential Decree.

² "Electronic Financial Service Provider" refers to an entity (excluding financial companies) that has obtained permission or completed registration in accordance with the provisions of Article 28.

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

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](#).

0.5

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Electronic Financial Transaction Act

Electronic Financial Transactions Act aims to clarify the legal relationships governing electronic financial transactions and lay a foundation for the sound development of the electronic financial industry, so as to deliver financial convenience to the public and contribute to national economic growth. To ensure the security and reliability of electronic financial transactions, the Act sets forth requirements for financial companies, electronic financial service providers and other relevant parties, including formulating plans concerning information security technologies, appointing a chief information protection officer, conducting regular vulnerability analysis and assessment of electronic financial infrastructure, and responding to and reporting infringement incidents in a timely manner.

In this chapter, Tencent Cloud will extract and summarize the control requirements relevant to cloud service providers under the Electronic Financial Transaction Act, and describe how Tencent Cloud, as a cloud service provider, assists financial companies, electronic financial service providers and other entities in complying with such requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
21	Duty to Ensure Safety	(1) A financial company, etc. shall fulfill its fiduciary duty of care in good faith so as to ensure safety in handling electronic financial transactions. (2) In order to ensure the safety and reliability of electronic financial transactions, a financial company etc. shall comply with the standards determined by the Financial Services Commission with respect to the information technology sector, such as human resources, facilities, electronic apparatus, and expenses for conducting electronic transmissions or processing, the electronic financial affairs and certification methods including the use of certificates under the Digital Signature Act. (3) The Financial Services Commission shall not compel the use of any specific technology or service when determining the standards referred to in paragraph (2) and shall endeavor to promote the fair competition of security technologies and certification	The customer shall comply with the relevant standards of the Financial Services Commission concerning information technology, electronic financial business, and electronic signature certificate authentication, manage and protect the security of electronic financial transactions, and formulate an annual information technology-related plan, which shall be verified and signed by its representative before submission to the Financial Services Commission. To support customers in complying with regulatory requirements, Tencent Cloud strictly abides by the laws and regulations of the jurisdictions where it operates, and has established security compliance-related procedures to ensure that information security operations meet the requirements of relevant laws, regulations, standards and procedures. Tencent Cloud's legal team continuously identifies and collects compliance requirements related to Tencent Cloud's business, compiles a corresponding list of laws and regulations, and maintains and updates it on a regular basis. Tencent Cloud undergoes annual independent professional audits by domestic and international third parties.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technologies.	Through System and Organization Controls (SOC) reports, Tencent Cloud provides assurance to cloud customers, independent auditors, regulators, shareholders, and other stakeholders regarding its latest internal control status.
		(4) For safe electronic financial transactions, the financial companies or electronic financial business entities prescribed by Presidential Decree shall annually establish a plan for the information technology sector and submit it to the Financial Services Commission after obtaining confirmation and signature of its or his or her representative, as prescribed by Presidential Decree.	In terms of information security management planning, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Management.
21-2	Appointment of Chief Information Security Officers	(1) Any financial company or electronic financial business entity shall appoint a chief information security officer to be responsible for managing electronic financial business and information technology security which forms the basis of electronic financial business. (2) A financial company or an electronic financial business entity prescribed by Presidential Decree in consideration of its or his or her total assets, number of employees, etc. shall appoint one of the executives (including any person prescribed in Article 401-2 (1) 3 of the Commercial Act) as a chief information security officer. (3) The chief information security officer of the financial companies or electronic financial business entities prescribed by Presidential Decree in consideration of its or his or her total assets, number of employees, etc. shall not concurrently perform duties in the information technology sector other than those referred to in paragraph (4). (4) A chief information security officer under paragraph (1) shall perform the following duties: - Establishing strategies and plans for securing the stability of electronic financial transactions under Article 21 (2) and protecting the users thereof; - Protecting the information	Based on factors such as its total assets and number of employees, the customer shall appoint a highest-ranking person in charge of information protection, who shall be fully responsible for the security management of electronic financial business and its underlying information technology, including the formulation of information security strategic planning, security-related human resources and budget management, accident prevention and emergency response, etc. To support customers in complying with regulatory requirements, Tencent Cloud has established an information security management system and appointed a Chief Information Security Officer to oversee information security governance comprehensively. The primary responsibilities include: - Leading the establishment, implementation, and continuous improvement of Tencent Cloud's information security management system, ensuring strict compliance with national laws, regulations, regulatory requirements, and industry information security standards; - Overseeing the performance evaluation and enhancement of the company's information security management system, driving the iterative improvement of security capabilities; - Ensuring the allocation of sufficient resources for information security management, organizing employee security awareness and capability training to meet information security management requirements;

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technology sector;	(4) Coordinating cross-departmental and cross-domain information security efforts to ensure the efficient operation of the system.
		3. Managing human resources and forming a budget, which are necessary for the security of the information technology sector;	
		4. Preventing electronic financial transaction accidents, and taking measures therefor;	
		5. Other matters prescribed by Presidential Decree for securing the stability of electronic financial transactions.	
21-3	Analyzing and Assessing Vulnerability of Electronic Financial Infrastructure	(1) To ensure the safety and reliability of electronic financial transactions, a financial company and an electronic financial business entity shall analyze and assess³ the following matters with respect to its or his or her electronic financial infrastructure⁴ and report⁵ the findings therefrom (referring to the findings from analysis and assessment of vulnerability, where conducted under Article 9 of the Act on the Protection of Information and Communications Infrastructure) to the Financial Services Commission: 1. Matters relating to the organization, facilities, and internal control of the information technology sector; 2. Matters relating to electronic	The customer shall conduct vulnerability analysis and assessment on electronic financial infrastructure, and formulate and implement necessary supplementary measure implementation plans based on the results. The customer shall promptly report the assessment results and supplementary measure implementation plans to the Financial Services Commission. For vulnerability scanning, Tencent Cloud offers the Vulnerability Scanning Service (VSS) to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation

³ According to Article 11-6 (2) of the Enforcement Decree of this Act, the analysis and assessment of vulnerabilities in electronic financial infrastructure shall be conducted at least once per business year.

⁴ "Electronic Financial Infrastructure" refers to information processing systems used for electronic financial transactions and information and communication networks specified in Subparagraph 1 of Paragraph 1 of the [Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.] .

⁵ In accordance with Article 11-6 (3) of the Enforcement Decree of this Act, a report on the results of the vulnerability analysis and assessment, along with an implementation plan for supplementary measures, must be submitted to the Financial Services Commission within 30 days of the completion of the analysis and assessment.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		apparatus and the means of access of the information technology sector; 3. Matters relating to measures to respond to infringements in order to maintain electronic financial transactions; 4. Other matters specified by Presidential Decree. (2) A financial company and an electronic financial business entity shall establish and implement a plan to take necessary complementary measures based on the findings from analysis and assessment of vulnerability in the electronic financial infrastructure under paragraph (1). (3) The Financial Services Commission may require public officials under its control to inspect the findings from analysis and assessment of vulnerability in the electronic financial infrastructure under paragraph (1) and the actual status of implementing complementary measures pursuant to paragraph (2).	advice to reduce security risks. VSS can integrate with other Tencent Cloud products such as Host Security and Web Application Firewall to achieve a closed-loop process from risk monitoring to risk mitigation. For penetration testing, Tencent Cloud offers the Penetration Testing Service (PTS), which fully simulates attack techniques and vulnerability exploitation methods commonly used by hackers. PTS uses controlled, non-destructive approaches to deeply probe the security of target systems, identify weaknesses in targets and network devices, and provide hardening recommendations to help customers improve system security. It also supports validation after vulnerability remediation. To support customers in complying with regulatory guidelines, Tencent Cloud has established an internal regular vulnerability scanning and penetration testing mechanism. Tencent Cloud's internal vulnerability scanning typically includes web vulnerabilities, component vulnerabilities, configuration scanning, etc. Vulnerability scanning tasks are automatically generated via the vulnerability scanning system to scan assets in the cloud environment, and discovered vulnerabilities are analyzed, classified, and remediated. In terms of penetration testing, Tencent Cloud's security team regularly conducts full-link large-scale penetration testing, and flexibly performs targeted penetration testing before new product launch or in the event of major changes. Test results are notified to relevant responsible departments via security work orders, and the responsible departments promptly patch vulnerabilities or implement other compensatory control measures to ensure that exploitable

No.	Domain	Summary of Controls	Tencent Cloud's Response
			vulnerabilities identified in penetration testing are properly addressed. In addition, Tencent Cloud regularly conducts red-blue team exercises to simulate defense against cyber-attacks. With regard to information technology-related organizations and internal controls, Tencent Cloud's security team conducts internal security audits at least once a year and continuously monitors the status of the cloud platform and internal systems to maintain a sound security posture and comply with relevant laws, regulations and security management standards. Furthermore, Tencent Cloud undergoes annual professional audits by independent third parties and discloses its latest internal control over service organizations to cloud user organizations, independent auditors, regulators, shareholders and other relevant stakeholders by providing assurance-based System and Organization Controls (SOC) reports.
21-5	Notification of Infringement Incidents	(1) If an incident, such as disturbance or paralysis of electronic financial infrastructure, occurs due to an electronic infringement (hereinafter referred to as "infringement incident"), the relevant financial company and electronic financial business entity shall, without delay, inform the Financial Services Commission thereof. (2) If an infringement incident occurs, the relevant financial company and electronic financial business entity shall analyze the causes thereof and take necessary measures to prevent the spread of	The customer shall analyze the cause of an infringement incident, take necessary measures to prevent damage from escalating, and immediately report the incident to the Financial Services Commission. To support customers in detecting and responding rapidly to incidents, Tencent Cloud provides Cloud Security Center (CSC), a one-stop security management platform. Through its Asset Center, Risk Center, Alert Center, Advanced Security Management and other functions, it helps customers achieve a closed-loop security operation covering threat detection before an incident, response and handling during an incident, and traceability analysis after an incident, improving the efficiency of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		damage.	security operations. To support customers in complying with regulatory guidelines, Tencent Cloud has formulated information security incident management specifications for incident response and handling, established information security reporting, response and handling mechanisms and relevant procedures, and clarified the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud records security incidents using an internal security operations system. For detected and identified security incidents, Tencent Cloud analyzes and classifies the incidents based on factors such as the nature of the incident, data sensitivity and scope of impact, and promptly notifies the responsible personnel to follow up and handle the incidents. To ensure the effectiveness and timeliness of the incident response process, internal business departments of Tencent Cloud regularly conduct drills related to information security incident emergency plans. Technical training is also provided to security team personnel in line with developments in security technology and trends, to ensure they understand and comply with the latest security regulations and operating procedures and master the latest information security standards and best practices. To support customers in effectively fulfilling their communication and notification obligations, Tencent Cloud has established procedures for information security incident response, escalation and notification to provide timely early warnings or notifications to internal personnel, customers and other relevant parties that may be or have been affected by

No.	Domain	Summary of Controls	Tencent Cloud's Response
			incidents, ensuring orderly, timely and efficient communication and coordination among all parties. For security incidents that may affect customers, Tencent Cloud will, after internal review based on the scope and severity of the information security incident, notify customers of the handling and analysis results of the information security incident through appropriate channels and provide corresponding technical support to assist customers in taking remedial measures to minimize losses.
26	Provision of Electronic Financial Transaction Information	No one who recognizes the existence of any of the following matters in the course of performing duties relating to electronic financial transactions shall provide or disclose such information to any third party or use it for any purpose other than his or her duties without the consent of the relevant user: Provided, That the same shall not apply to cases provided for in the proviso of Article 4 (1) of the Act on Real Name Financial Transactions and Confidentiality or in any other statute: 1. The matters relating to the identity of the user; 2. The information or materials relating to the accounts, the means of access, and the details and results of electronic financial transactions of the user.	Tencent Cloud strictly adheres to laws and regulations governing user privacy and data security in all jurisdictions where it operates, has established a comprehensive information security and privacy protection management system, and has obtained a number of international standard certifications. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive 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). In addition, for more information regarding the collection, processing and sharing of personal information by Tencent Cloud, please refer to the Privacy Policy.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Regulation on Supervision of Electronic Financial Transactions

The [Regulation on Supervision of Electronic Financial Transactions](#) is issued by the Financial Services Commission (FSC) and primarily clarifies three key areas, including:

1. Matters delegated to the Financial Services Commission under the "Electronic Financial Transactions Act" and its enforcement decree;
2. Implementation of the requirements specified in the "Electronic Financial Transactions Act" and its enforcement decree;
3. Other necessary matters stipulated by laws and regulations, as well as those required for the information technology departments of institutions supervised by the Financial Supervisory Service to ensure their security.

Article 14-2 of the Regulations sets forth requirements for financial companies and electronic financial service providers in the ROK with respect to the use and assessment of cloud computing services. It provides relevant evaluation items and corresponding criteria through: Appendix 2-2 Standards for Evaluating the Soundness and Safety of Cloud Computing Service Providers; Appendix 2-3 Task Continuity Plan for the Use of Cloud Computing Services; Appendix 2-4 Safety Measures for the Use of Cloud Computing Services.

In this chapter, Tencent Cloud will extract and summarize the provisions relevant to cloud service providers under the Regulation on Supervision of Electronic Financial Transactions, and describe how Tencent Cloud, as a cloud service provider, assists financial companies and electronic financial service providers in complying with such requirements.

6.1 Securing the Safety of Electronic Financial Transactions and Protecting Users

6.1.1 Personnel, Organization and Budget

No.	Domain	Summary of Controls	Tencent Cloud's Response
8	Personnel, Organization and Budget	(1) Each financial company and electronic financial business operator shall abide by the following matters in the management of his/her or its personnel and organizations: 1. Securing an organizational structure to take exclusive charge of his/her or its information processing system and electronic financial affairs; 2. Securing an in-house organizational structure and personnel to review the appropriateness of contracts for other reserve personnel; 3. Offering education and training programs to upgrade the quality of	The customer shall formulate and implement training programs to enhance the information protection capabilities of executives and employees, evaluate the implementation of such programs and employees' compliance with information security-related laws and regulations, and supplement or update the programs as necessary. The customer shall establish and implement procedures for imposing sanctions on employees who violate information security-related laws and regulations. The customer shall also have personnel with professional expertise in information technology and information protection, as well as sufficient budget. In terms of information security management organizational structure, Tencent Cloud has established cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		his/her or its IT personnel and train other reserve personnel; 4. The chief executive shall evaluate the results of the implementation of the training plan for the previous year, and the chief information protection officer shall reflect those results in the training plan for this year 5. The chief information security officer shall conduct regular inspections as to whether executives and employees comply with laws and regulations related to information security and report the results of such inspections to the chief executive officer. 6. The chief executive officer shall formulate and administer detailed standards and procedures for sanctions on violations of laws and regulations related to information security committed by executives and employees. (2) Each financial company and electronic financial business operator shall have adequate personnel and budgets with expertise in the fields of information technology and information protection.	security and information security-related organizational frameworks, clearly defining security functional roles and responsibilities at different levels, and outlining mechanisms for information security auditing and risk assessment. Tencent has set up a Security Technology Committee and various specialized security teams with distinct functions and areas of expertise. Internally, the company has developed comprehensive human resources management standards and procedures to ensure that recruitment and staffing align with job requirements. Tencent Cloud has also assembled a team of industry-leading expert services dedicated to providing customers with secure, reliable, professional, and compliant products and services. In terms of training and education, 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 basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.
8-3	Separation of Duties	Financial institutions or e-finance providers shall establish and operate separation of duties standards for internal control of the information technology sector.	The customer shall establish and implement segregation of duties standards for internal control within the information technology department. To support customers in complying with regulatory requirements, Tencent Cloud has established cloud security and information security-related organizational structures. Based on principles such as the separation of duties, the company has clearly defined security functional roles and responsibilities at different levels, ensuring the segregation, mutual constraints, and oversight of incompatible positions. This includes, but is not limited to, the separation of system development and operational maintenance, the separation of business operations and system approvals, and so on.

6.1.2 Facility

No.	Domain	Summary of Controls	Tencent Cloud's Response
9	Matters Relating to Buildings	Financial companies or e-finance providers shall establish and operate security measures and access control security measures for the building where the computer room is located.	The customer shall formulate and implement measures to safeguard the security of the building housing the computer room and control access thereto. Tencent Cloud's global data centers are selected, constructed or leased in accordance with relevant international standards and local security requirements, with full consideration of environmental threats to avoid areas with high probability of environmental risks. Currently, Tencent Cloud has deployed two leased data centers in South Korea. To ensure the resilience and security of data centers, Tencent Cloud has established a rigorous management system

No.	Domain	Summary of Controls	Tencent Cloud's Response
			covering the entire process from vendor access, contractual restrictions to continuous monitoring. Tencent Cloud is committed to providing customers with a secure, stable, sustainable and reliable physical infrastructure foundation, and has formulated formal physical security management policies to standardize operational safety, timely identify risks and strengthen physical security management. In terms of physical access control, Tencent Cloud requires data center operators to establish a complete personnel access control security matrix in the access authorization system based on personnel categories and access permissions, so as to achieve effective control over the access and operations of all types of personnel. Tencent Cloud requires operators to verify the identity and check personal belongings of all visitors or staff entering and exiting the data center, and register the items carried. In terms of security and monitoring, Tencent Cloud requires operators to assign security personnel to conduct inspections of each computer room and equipment in strict accordance with inspection checklists and schedules, sign and record the inspection time at each checkpoint, and immediately activate the data center emergency response procedure once infrastructure failures or security incidents are detected. Tencent Cloud also requires operators to equip data centers with a 24/7 non-blind-spot video surveillance and alarm system, staffed by security personnel on duty, with surveillance recordings securely stored and retained for a sufficient period.
10	Matters Relating	A financial company or an	The customer shall formulate and

No.	Domain	Summary of Controls	Tencent Cloud's Response
	to Facilities, such as Power Supply System and Air Conditioning System	electronic financial business entity shall establish and operate standards for the safety of facilities, such as power supply and air conditioning, in the building where the computer room is located.	implement safety standards for facilities such as power supply and air conditioning within the building housing the computer room. To support customers in complying with regulatory requirements, Tencent Cloud has established physical security management policies to standardize operational safety, identify risks in a timely manner, and strengthen physical security management. Tencent Cloud's global data centers are sited, constructed, or leased in accordance with relevant international standards and local security requirements. Currently, Tencent Cloud has deployed two leased data centers in South Korea. Tencent Cloud requires data center operators to adopt highly stable, fully redundant power supply systems and air conditioning systems to avoid any impact on the continuity and availability of the data center caused by single points of failure.
11	Matters Relating to IT Room	A financial company or e-finance provider shall establish and operate measures with respect to the computer room, including the following provisions: 1. Computing rooms and disaster recovery centers of domestic financial companies or e-finance providers shall be installed in the country (except for electronic payment agents for foreign cybermalls registered in accordance with Article 50, Paragraph 2). 2. Will not install wireless network 3. Other matters concerning the safety and security of computer rooms, such as disaster prevention	The customer shall locate its computer rooms and disaster recovery centers within South Korea, and protect the security of the computer rooms through disaster prevention, access control and other measures. Tencent Cloud builds or leases data centers in multiple regions around the world in accordance with relevant international standards and local security requirements, providing customers with multi-region and multi-zone options. It strictly complies with the laws and regulations on user privacy and data security protection in the jurisdictions where it operates, and continuously and proactively tracks local regulatory developments. Customers may independently and flexibly deploy their data and systems in different

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and relief, access and access control	regions or availability zones based on business development needs and data security requirements. Currently, Tencent Cloud has two data centers in South Korea, offering a variety of cloud computing services including cloud servers, cloud databases, cloud storage and others. Korean customers may choose to store, process and back up their data locally in Korea. In terms of disaster prevention, Tencent Cloud requires operators to equip data centers with a complete fire protection system, including regional fire detection systems, automatic fire extinguishing systems and manual fire-fighting devices for emergency use. Tencent Cloud also requires operators to configure data centers with lightning protection systems, anti-radiation systems, power supply and distribution systems, UPS systems, lighting systems and other facilities necessary to maintain normal operation of the computer rooms. It further requires data center maintenance personnel to work in shifts to ensure round-the-clock maintenance and support for the prompt resolution of equipment failures. And the installation of wireless telecommunication networks is prohibited in the production environment. In terms of access management for secure areas, Tencent Cloud requires data center operators to establish a complete personnel access control security matrix in the access authorization system based on personnel categories and access permissions, so as to achieve effective control over the access and operations of all types of personnel. Tencent Cloud requires operators to verify the identity and check personal belongings of all visitors or staff entering and exiting the data center, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			register the items carried.

6.1.3 Information Technology

No.	Domain	Summary of Controls	Tencent Cloud's Response
12	Measures to Protect Terminals	Each financial company and electronic financial business operator shall abide by the following to protect his/her or its terminals: 1. Taking measures to prevent anyone other than responsible staff from accessing the terminals without authorization. 2. Keeping records that make it possible to verify whether terminals accessing the information processing system are used by persons authorized to use them. 3. Designating major terminals to which more intense protective measures are applied, such as prohibiting their removal out of the premises, logging on to the Internet, and the logging on to groupware and regular verification of malicious code infection. 4. Controlling access to auxiliary memory devices or portable computer equipment from terminals so as to prevent divulgence of information, malicious code infections, etc.	The customer shall protect endpoints by maintaining system access records, restricting device usage to authorized users only, implementing enhanced protection measures for critical endpoints, and controlling access to auxiliary storage media on endpoints. The customer may adopt Cloud Workload Protection Platform (CWPP) to provide security protection for cloud hosts. Based on massive, accumulated threat data and machine learning, CWPP provides customers with security protection services such as hacker intrusion detection and vulnerability risk alerts, including functions like password crack blocking, abnormal login alerts, Trojan file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by current servers. To support customers in complying with regulatory requirements, in terms of host terminal protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to provide comprehensive monitoring and control of all server endpoint assets. The EDR solution supports antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing of command operations and login activities. It triggers alerts upon detecting malicious programs or abnormal behaviors, and Tencent Cloud follows up and handles these alerts through its ticketing system. For office endpoint protection, Tencent Cloud has formulated internal software

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
13	Measures to Protect Computer Data	(1) Each financial company and electronic financial business operator shall establish and implement measures to protect computer data in order to prevent the divulgence, destruction, etc. of such data, including the following: 1. Appropriate access management and control procedures shall be established and operated. 2. Managing the status of computer data held, and designating and managing the responsible person. 3. Controlling the carrying of computer data and computer equipment out of or into the premises. 4. Establishing and implementing a plan to safely carry out and urgently destroy auxiliary memory devices and other computer data in an emergency; 5. Regularly checking the status of	The customer shall establish and implement computer data protection measures, including access control procedures, data storage monitoring and protection measures, data transmission protection measures, data secure destruction measures, relevant emergency response plans, storage medium protection measures, backup and backup verification measures, and system operation records, and shall prevent the use of user information in testing. In addition, the customer shall establish and implement appropriate control measures for information processing system administrators who have access to endpoints and computer data, and review and supervise the principal work activities of such administrators. In terms of data access management, Cloud Access Management (CAM) helps customers securely and finely manage access to Tencent Cloud products and resources, granting specific permissions to different personnel for different resources. Customers can also monitor, conduct

No.	Domain	Summary of Controls	Tencent Cloud's Response
		auxiliary memory devices held and the management thereof with confirmation by the responsible person;.	compliance checks, operational audits and risk audits on Tencent Cloud account activities via CloudAudit . 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 users are granted the minimum permissions necessary to access assets and complete work tasks.
		6. Regularly backing up computer data according to their priority levels for putting the backup files in a remote safe deduplication storage, and keeping and managing a record of the backup files;.	
		7. Regularly verifying major backup files of computer data.	Customer data is classified as high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud will not attempt to access or disclose customer content. To ensure the control of employee access to cloud environments and infrastructure, bastion hosts have been fully deployed in Tencent Cloud's production environment to centrally control the administrator account permissions and account activities of Tencent Cloud backend system components. Background operation and maintenance logs are centrally stored in a log platform and regularly reviewed by Tencent Cloud's internal audit team.
		8. Controlling inquires into and outputting of user information and prohibiting any tests using such information (Provided, That tests using information of users who are juristic persons shall be allowed when the consent of the users is obtained as prescribed by the Governor of the Financial Supervisory Service, and if the use of user information is essential to conduct load testing, etc., such information shall be used after being converted and shall be deleted immediately after the completion of such testing).	In terms of data storage protection , many Tencent Cloud storage and database products support data encryption using secure high-strength encryption algorithms and support full lifecycle key management and protection to ensure data confidentiality. Tencent Cloud adopts multi-copy redundant storage and erasure coding technology for stored data and takes necessary recovery measures when integrity errors are detected, greatly improving data fault tolerance.
		9. The operation records of the information processing system shall be automatically recorded and maintained by the Director of the Financial Supervisory Service regardless of whether the connection is successful or not and shall be preserved for at least one year.	
		10. Prohibiting the retention of user information and other important information in terminals and the sharing of terminals	In terms of data transmission protection , all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(Provided, That if retention of such information in terminals is essential, it shall be subject to approval by the responsible person after specifying the reasons for and period of retention, administrator password, etc.); 11. If a user is subject to a personnel change, such as transfer of post or retirement, immediately controlling the user's access to the information processing system in such a manner as to delete, or suspend the use of, his/her user account or to change a user account shared with him/her. (2) If sharing a user account is inevitable, the details of access shall be recorded and managed for each individual. (3) Each financial company and electronic financial business operator shall establish and implement appropriate measures to manage a data processing system administrator authorized to access terminals and computer data: Provided, That any activity performed by the data processing system administrator in relation to his/her major duties shall be cross-checked and monitored by the responsible person pursuant to Article 28 (2).	HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • <u>Direct Connect (DC)</u>: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • <u>VPN Connection</u>: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. For data deletion and destruction, after a customer's service is terminated, Tencent Cloud will follow strict data erasure methods to completely delete customer data including copies and backups after the retention period expires, and the deleted data cannot be recovered. In terms of media management, Tencent Cloud has established relevant procedures, clearly defining specific processes and standards for media storage and media disposal. Media disposal must undergo relevant approval before it is carried out, and proper records of the disposal process must be maintained. When transmitting information using physical media, Tencent Cloud employs a work order system to track the entire process of media retrieval, transportation, and return throughout the workflow. In terms of data backup, Tencent Cloud has formulated backup management

No.	Domain	Summary of Controls	Tencent Cloud's Response
			procedures to back up important data collected and processed in accordance with relevant legal and regulatory requirements. For internal important information, Tencent Cloud formulates backup strategies based on data levels and regularly conducts recovery tests. For cloud customer data, Tencent Cloud provides multi-storage copies and backup services according to the functions of cloud products or services, and assumes responsibility for the provided data backup services in accordance with the service level agreements of the products. Various cloud products/services provided by Tencent Cloud, including computing services, network services, storage services, database services, container and middleware services, are highly available and can help customers achieve high availability of systems or services, such as: • <u>Cloud Load Balancer (CLB)</u> provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Cloud Object Storage (COS)</u> provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource

No.	Domain	Summary of Controls	Tencent Cloud's Response
			isolation for Customer data to ensure durability. • <u>Cloud Native Database TDSQL-C:</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 reliability and availability with robust automatic backup and lossless recovery mechanisms. • <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data. Regarding the security management of test data, 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. For system operation or operation records, Tencent Cloud provides <u>Cloud Log Service (CLS)</u> for customers. As a one-stop log service platform, CLS supports log collection, storage, retrieval and analysis, real-time consumption, log delivery and other services, assisting customers in business operation, security monitoring, log audit and log analysis. CLS allows users to customize the log retention period: Standard storage log topics can be retained for 1 to 3600 days or permanently;

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Infrequent access log topics can be retained for 7 to 3600 days or permanently. In terms of endpoint management, Tencent Cloud has deployed Data Loss Prevention (DLP) tools on employee work terminals to restrict the export of data externally, thereby monitoring, detecting, and preventing potential data theft activities. Regarding account permission changes, Tencent Cloud maintains records of personnel identity information corresponding to job roles and permission levels of various business systems and conducts regular internal permission reviews to ensure permission is not abused or misused. Appropriate follow-up actions will be taken for access permissions that are no longer required, and unnecessary access permissions will be revoked in a timely manner.
14	Measures to Protect Information Processing System)	For the safe operation of the information processing system, the financial company or e-finance operator shall establish and operate protective measures, including the following: Operation Manual, Maintenance Manager, List of Responsible Persons and Disability Records Department. 1. Create and store each of the following items A. Operating Manual for Major Information Processing Systems B. Director of Maintenance Management who recorded the implementation of regular maintenance for major information processing systems C. Department of Persons	The customer shall establish and maintain operation manuals, maintenance management ledgers, list of responsible persons, and fault records for major information processing systems, continuously monitor the status of system resources, and promptly install critical patches. The customer shall also back up configurations of information processing systems and implement control measures such as two-factor authentication and operation audit for administrator logins to information processing systems. 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,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Responsible for Information Processing Systems and Disability Situation Registry.	ports, processes, and applications. 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. Tencent Cloud provides Bastion Host (BH) to assist customers in user management, authorization management, authentication management
		2. Building a monitoring system to monitor, issue warning against, and control the state of the system resources, which will help ascertain whether the information processing system functions normally;	and comprehensive audit. Bastion Host can provide different authentication methods for different users according to actual scenario needs, such as static passwords, LDAP, etc. To enhance security, Tencent Cloud Bastion Host supports two-factor authentication for users.
		3. Establishing and complying with control procedures to prevent information processing system failures due to any errors, etc. at the time of integrating, converting or redeveloping the system.	Tencent Cloud has internally formulated information asset management specifications and full lifecycle management processes to classify, grade, manage and protect assets including electronic data, hardware and virtual devices, infrastructure, application systems and software. Tencent Cloud manages hardware equipment and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset retirement and replacement, to ensure stable operation of the underlying cloud platform and provide reliable support for business systems.
		4. Installing quickly any important patches urgently required in relation to the operating system, utilities, etc. of the information processing system;	In terms of service level and monitoring of cloud products/services, Tencent Cloud
		5. Regularly backing up the operating systems, details of configuration, etc. of the information processing system according to their priority levels and putting the backup files in a remote safe deduplication storage, and keeping and managing a record of the backup files for at least one year;	
		6. Implementing mandatory procedures for additional authorization in addition to the account and password in cases of logging into the account of the operating system of an information processing system. Establishing a regular monitoring system on the rights of use, records of access, details of work, etc. on the account	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		of the operating system of an information processing system, and taking necessary control measures immediately when strange symptoms appear.	delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. Tencent Cloud also provides <u>Tencent Cloud Observability Platform (TCOP)</u> to assist customers in monitoring cloud products/services. TCOP collects and displays various monitoring metrics reported by cloud products such as CVM and TencentDB, as well as customer-customized metrics through visual charts, helping customers grasp resource utilization, application performance and operation status of cloud products in real time. TCOP supports setting alerts for indicators and notifies customers of business exceptions in a timely manner through message push according to the configured alert rules. In terms of Change and Operations Management, Tencent Cloud has formulated operation and maintenance (O&M) management specifications to provide guidelines and requirements for daily O&M activities. Tencent Cloud adopts mature tool-based and automated O&M management platforms to manage O&M operations, and strictly controls change time windows through internal O&M mechanisms to ensure O&M requests are completed within the specified time. Tencent Cloud has also set detailed O&M security "red lines" and regularly conducts internal O&M security reviews.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			To ensure controllability and traceability of operations in the production environment, background O&M operation records are fully documented and centrally stored in a log platform, and Tencent Cloud's internal audit team regularly investigates and traces suspicious operations during O&M. In terms of patch management, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Regarding offsite backup and disaster recovery requirements, different regions of Tencent Cloud are completely isolated to ensure maximum stability and fault tolerance across regions. Each region is further divided into multiple isolated availability zones to guarantee business continuity for customers. Currently, Tencent Cloud has deployed two leased data centers in South Korea. Customers may independently and flexibly deploy data and systems in different regions or availability zones according to business development and data security requirements, and adopt different business continuity modes to meet disaster recovery requirements.
14-2	Procedures for Use of Cloud Computing Services	(1) Where a financial company or an electronic financial business entity intends to use cloud computing services under subparagraph 3 of Article 2 of the Act on the Development of Cloud Computing and Protection of Its Users, the entity shall undertake the following procedures: 1. Evaluation of the importance of	The customer shall, prior to using cloud computing services, assess the importance, characteristics, disruption impact and concentration risks of the business processed through cloud computing services, as well as the security of the cloud service provider, and formulate and implement business continuity plans and security safeguards related to the use of cloud computing services. In addition, the customer shall promptly report to the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		tasks using cloud computing services based on the following criteria: (a) The characteristics of the tasks, including scale and complexity, which are processed through the cloud computing service; (b) The impact of service interruptions from the cloud computing service provider; (c) The impact of electronic breaches on customers; (d) Dependency risk when entrusting multiple tasks to the same cloud service provider; (e) The internal control capacity of the financial company or electronic financial business entity to manage the use of cloud computing services and ensure compliance with applicable laws and regulations; and (f) Other matters determined and publicly announced by the Governor of the Financial Supervisory Service. 2. Evaluation of the soundness and safety of the cloud computing service provider (For tasks classified as non-critical, only the required items in Attached Table 2-2 can be assessed); 3. Development and implementation of task continuity plans and safety measures for cloud computing service usage (For tasks classified as non-critical under subparagraph 1, only essential measures outlined in Attached Tables 2-3 and 2-4 can be developed and implemented). (2) The evaluation results, task continuity plans, and safety measures under Paragraph (1) must be reviewed and approved by	Financial Supervisory Service when entering into a new service contract with a cloud service provider, or when a material change or incident occurs with the cloud service provider. To support customers in evaluating cloud service providers, Tencent Cloud will provide relevant information upon customer request and assign dedicated personnel to actively respond to and cooperate with customers' due diligence activities. The following is an overview of Tencent Cloud's practices as a cloud service provider in responding to due diligence requirements across various aspects: • Reputation: As a cloud computing brand under Tencent, a leading enterprise in China's internet industry, Tencent Cloud has obtained multiple professional certifications from industry organizations, provides comprehensive cloud solutions, and has delivered reliable services to numerous enterprises and government agencies. • Professional and technical capabilities: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the Information Security Committee established under Article 8-2. (3) A financial company or electronic financial business entity may perform the evaluation under Paragraph (1)2 itself or use the results of the assessment conducted by the computer security incident response agency under Article 37-6(1). (4) A financial company or electronic financial business entity must report the following events to the Governor of the Financial Supervisory Service within three (3) months of their occurrence, along with supporting documents, reasons, and response plans: 1. When signing a new cloud computing service agreement; 2. When significant changes to the cloud computing service provider, such as mergers, splits, transfer of contractual status, or re-entrustment occur; 3. When a cloud computing service provider fails to fulfill important contractual obligations related to maintaining service quality and ensuring safety, etc.; 4. When substantial changes concerning Paragraphs (1)2 or 3 occur. (5) Reports filed with the Governor of the Financial Supervisory Service under Paragraph (4). (6) If the Governor of the Financial Supervisory Service identifies omissions in the report submitted	ensuring reliable and continuous service for customers. Compliance capabilities: Tencent Cloud strictly complies with the laws and regulations of the jurisdictions where it operates and has established security compliance-related procedures to ensure that information security operations meet the requirements of relevant laws, regulations, standards and procedures. Tencent Cloud conducts security testing, risk assessment and internal audit of its information systems on an annual basis to ensure that security defense capabilities remain at a reasonable level and comply with relevant security management standards and requirements. The security team continuously conducts internal and external security audits of Tencent Cloud's security management system each year to verify the effectiveness and compliance of information security measures. For South Korea, Tencent Cloud has obtained the Korean Information Security Management System (K-ISMS) certification and undergoes regular annual audits by the Korea Internet & Security Agency (KISA). Business continuity and disaster recovery: Tencent Cloud has obtained the international standard certification of ISO/IEC 22301 Business Continuity Management Systems. To ensure the continuous availability of customers' businesses, Tencent Cloud has developed detailed disaster recovery plans for its cloud products and conducts regular

No.	Domain	Summary of Controls	Tencent Cloud's Response
		under Paragraph (4), or deems the task continuity plan or safety measures inadequate, the Governor may require the financial company or electronic financial business entity to improve or supplement the submitted report or plan/measures. (7) Article 11(1)(2) and Article 15(1)5 do not apply to computer rooms hosting the data processing system of a compliant cloud computing service provider under Paragraph (1). However, if a financial company or electronic financial business (excluding domestic branches of foreign financial companies that do not significantly impact the safety and reliability of electronic financial transactions, and electronic payment settlement agencies for overseas cybermalls as set forth in Article 50-2) processes personal identification information or credit information through cloud services, Article 11(2) shall apply, and the data processing system must be located within Korea. (8) Other matters regarding the use of cloud computing services by financial companies or electronic financial business entities shall be governed by the Regulation on Information Processing Business Delegation of Financial Companies.	drills in strict accordance with requirements to guarantee the timeliness and feasibility of such plans. Risk management: Tencent Cloud develops and maintains an internal risk management framework in accordance with ISO/IEC 27001:2022 to identify, analyze and manage identified risks. Tencent Cloud performs formal risk assessments regularly, drawing on risk sources including industry security incident reports, Tencent Cloud's accumulated practices, and risk databases of professional institutions to identify risks in Tencent Cloud's products and service processes. Tencent Cloud assesses asset value, risk likelihood and impact severity to calculate risk levels. Based on risk analysis results, it provides response strategies and corresponding mitigation measures for identified risks to reduce risks to an acceptable level. Audit and assessment: Tencent Cloud undergoes regular professional audits by independent third parties and discloses its latest internal control over service organizations to cloud user organizations, independent auditors, regulators, shareholders and other relevant stakeholders by providing assurance-based System and Organization Controls (SOC) reports. For South Korea, Tencent Cloud has obtained the Korea Information Security Management System (K-ISMS) certification. In addition, Tencent Cloud actively responds to and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			cooperates in audits or assessments initiated by customers.
			For more information regarding Tencent Cloud's security, business continuity plans and security safeguards, please refer to Section 6.4 "Standards for Evaluating the Soundness and Safety of Cloud Computing Service Providers" , Section 6.5 "Task Continuity Plan for the Use of Cloud Computing Services" , and Section 6.6 "Safety Measures for the Use of Cloud Computing Services" .

6.1.4 Information Protection

No.	Domain	Summary of Controls	Tencent Cloud's Response
15	Anti-Hacking Measures	(1) Each financial company and electronic financial business operator shall establish and implement the following measures to protect the information processing system and information communications network against any hacking or other electronic trespass: 1. Establishing and operating an information protection system to prevent accidents due to any hacking and other electronic trespass; 2. Immediately installing any urgent and important patches related to system programs, etc. to prevent any hacking or other electronic trespass; 3. Separating, blocking, and prohibiting internal business systems connected to internal communication networks from connecting to external communication networks, such as the Internet (including wireless	The customer shall adopt protective measures to prevent information processing systems and information and communication networks from cyberattacks and other electronic intrusions, including the timely installation of critical emergency patches and the isolation of internal networks from the Internet, and shall assign responsible persons for such measures and keep records of implementation results. The customer shall also implement security measures when installing and operating wireless networks to prevent unauthorized access via wireless networks. For network segmentation or partitioning, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can

No.	Domain	Summary of Controls	Tencent Cloud's Response
		networks): Provided, that this shall not apply to the following cases: (a) Research and development activities that do not process users' unique identification information or personal credit information (However, this is only applicable if a financial company or electronic financial business entity has conducted its own risk assessment and applied the network separation alternative information protection control set by the Governor of the Financial Supervisory Service); (b) Situations deemed inevitable for business purposes and confirmed by the Governor of the Financial Supervisory Service.	configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. 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.
		4. Integrating and minimally performing functions distributing files in the internal communications network, and verifying the integrity of files where files are distributed;	
		5. Physically separating the information processing system located in computer rooms and the terminals directly connected for operation, development, and security purposes from any external communication networks, such as the Internet: Provided, that this shall not apply to the following cases: (a) Research and development activities that do not process users' unique identification information or personal credit information (However, this is only applicable if a financial company or electronic financial business entity has conducted its own risk assessment	For secure network communication, customer interactions on the Tencent Cloud console are encrypted using HTTPS. VPN Connection enables secure transmission between on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet Key Exchange) and IPsec protocols to encrypt data, creating a secure and trusted channel over the Internet. For tenant isolation, Tencent Cloud enforces resource access control at the virtualization layer, private network isolation policies, web console permission management, identity verification, and secure API session handling. These mechanisms ensure that each customer can only access their purchased resources,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and applied the network separation alternative information protection control set by the Governor of the Financial Supervisory Service); (b) Situations deemed inevitable for business purposes and recognized by the Governor of the Financial Supervisory Service. (2) The matters prescribed by the Director of the Financial Supervisory Service shall be observed for the safe operation of the information protection system under paragraph (1) 1. (3) A responsible person shall be designated and managed for the information protection system referred to in any subparagraph of paragraph (1), and the results of operation thereof shall be preserved for at least one year. (4) Each financial company and electronic financial business operator shall take appropriate measures to promptly cope with damage caused by any hacking or other electronic trespass. (6) When installing and operating a wireless communications network, each financial company and electronic financial business operator shall abide by the following: 1. Minimizing the scope of affairs conducted using a wireless communications network, which shall be designated in advance with approval from the chief information security officer designated under Article 21-2 of	effectively preventing cross-tenant data access or tampering. For the internal network security protection and management of Tencent Cloud, Tencent Cloud has established network defence-in-depth architecture. Security domains are defined based on business functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time. In terms of Internet browsing security, the Tencent Cloud network team has adopted various protective measures, Tencent Cloud's network team has implemented multi-layered protective measures, including unified control of internet browsing channels, enabling web security filtering and malicious URL blocking, deploying endpoint security and antivirus software, and providing employees with security awareness training for safe internet browsing. In terms of wireless network management, Tencent Cloud has enabled security policies for wireless networks, requiring employee authentication for wireless network access. At the same time, the enterprise IT management console monitors wireless SSIDs and APs; if unauthorized SSIDs or APs are detected, alerts are sent to relevant IT administrators for handling. In terms of patch management, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the Act; 2. Establishing security measures, such as user authentication and encryption, to prevent illegal access via a wireless communications network; 3. Building a firewall to block the information processing system connected to the internal network of a financial company from accessing a wireless communications network except for designated business purposes and in designated zones; and operating a real-time monitoring system therefor; and regularly checking whether or not any unauthorized wireless access point (AP) is installed or connected and any important information is exposed. (7) Each financial company and electronic financial business operator shall establish measures to control access through his/her or its terminal to any program or Internet site unrelated to his/her or its business that contains obscene or gambling content.	patches trigger automated alerts.
16	Measures to Prevent Malicious Code Infections	Each financial company and electronic financial business operator shall establish and implement measures to prevent malicious code infections, promptly take necessary measures to minimize the spread of and damage from the malicious code.	The customer shall formulate and implement measures to prevent the infection and spread of malicious software. The customer may adopt Cloud Workload Protection Platform (CWPP) to provide security protection for cloud hosts. Based on massive, accumulated threat data and machine learning, CWPP provides customers with security protection services such as hacker intrusion detection and vulnerability risk alerts, including functions like password crack blocking, abnormal

No.	Domain	Summary of Controls	Tencent Cloud's Response
			login alerts, Trojan file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by current servers. To support customers in detecting and responding rapidly to incidents, Tencent Cloud provides Cloud Security Center (CSC), a one-stop security management platform. Through its Asset Center, Risk Center, Alert Center, Advanced Security Management and other functions, it helps customers achieve a closed-loop security operation covering threat detection before an incident, response and handling during an incident, and traceability analysis after an incident, improving the efficiency of security operations To support customers in complying with regulatory requirements, in terms of host terminal protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to provide comprehensive monitoring and control of all server endpoint assets. The EDR solution supports antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing of command operations and login activities. It triggers alerts upon detecting malicious programs or abnormal behaviors, and Tencent Cloud follows up and handles these alerts through its ticketing system. For office endpoint protection, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
17	Measures to Manage Open-Source Web Servers	(1) Each financial company and electronic financial business operator shall establish and implement appropriate measures to ensure safe management of his/her or its open-source web servers, including the following: 1. Ensuring that an open web server is established within an independent communications network (hereinafter referred to as "DMZ") between his/her or its internal and external communications networks to protect it as a means of network and web access control; 2. Assigning user accounts available for an open-source web server only to business-related persons, and adopting an additional means of authentication, in addition to IDs and passwords; 3. Restricting the use of services and testing and development resources, other than those provided through an open-source web server; and prohibiting the storage and management of user information and other important information within a DMZ (but do not, for managing transaction log cases as an exception to encrypt a	The customer shall formulate and implement appropriate measures to safeguard the security of public network servers, including isolating public network servers from the internal communication network, implementing access control and two-factor authentication for public network servers, and establishing and adopting information leakage prevention measures. The customer shall also restrict the storage and management of important information (such as user information) in the DMZ zone. Customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. Meanwhile, Tencent Cloud supports access permission management for private networks through Cloud Access Management (CAM), for example, controlling user access permissions to private networks via identity management and policy management. In addition, Cloud Firewall (CFW) provides customers with protection at different network boundaries, meeting the security and management requirements of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		unique identifying information must be separate security measures and other user information is established to manage storage); 4. Each financial company and electronic financial business operator shall take measures for the procedures and contents of Posting data on a web server for disclosure, and security measures to prevent the leakage, forgery, or falsification of personal information.	unified access control and log audit on the cloud. It supports proactive firewall ACL control, real-time IPS blocking, virtual patching, and malware detection; integrating Tencent threat intelligence to block abnormal outbound connections from hosts in real time. It can fulfil the DMZ zone requirements in traditional networks, focus on protecting core assets, and achieve fine-grained isolation and control between VPCs. Tencent Cloud has also established strict internal network isolation rules, realizing complete isolation between Tencent Cloud's internal office network and the production environment where customer data resides through physical and logical isolation. Tencent Cloud has fully deployed bastion hosts in the production environment to prevent unauthorized access. Furthermore, Tencent Cloud has internally deployed a network monitoring system to monitor and alert network devices such as routers, firewalls, and network servers. Through multiple measures including permission control and approval processes, unauthorized personnel are strictly prohibited from accessing internal network resources.
18	Measures to Manage IP Addresses	Each financial company and electronic financial business operator shall establish and implement appropriate measures, including those related to the address system, allocation, and management, to ensure the secure use of information provider addresses (hereinafter referred to as "IP addresses"), and shall keeping and preserving a separate record that indicates the details of Internet access using his/her or its	The customer shall take measures to ensure the secure use of IP addresses and separately record and store the Internet access status of internal and external IP addresses for at least one year. Customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical

No.	Domain	Summary of Controls	Tencent Cloud's Response
		internal and external IP addresses, for at least one year;	infrastructure, ensuring complete isolation between private networks. Tencent Cloud has established an internal IP management system for IP address planning, application, query, modification, and other related tasks. The allocation of both internal and external IP addresses must go through an application and approval process, with assignments centrally managed by network administrators. The IP management system maintains an IP address inventory and logs all internet access activities for internal and external IPs, including access timestamps, source IPs, destination IPs, port numbers, and other details, thereby meeting security audit requirements.
19	Key Management	(1) To prevent the distribution and misuse of encryption programs, financial companies or electronic financial service providers shall designate a responsible person for such programs, prohibit unauthorized use by any person other than the responsible person, and store the source program separately. (2) Financial companies or electronic financial service providers must establish procedures and methods for the injection, operation, renewal, and destruction of keys (including passwords or keys of authentication systems, etc., used to verify the authenticity and integrity of programs) applicable to cryptographic and authentication systems, and manage these keys securely.	The customer shall establish and implement procedures related to key lifecycle management and restrict access to the original encryption programs. Tencent Cloud provides Key Management Service (KMS) to assist customers in achieving full lifecycle management of encryption keys, ensuring that keys securely complete a series of operations including generation, storage, distribution, import, export, usage, recovery, archiving and destruction to prevent key leakage. Customer Master Key (CMK) is the core resource in KMS. As a primary key belonging to the customer, CMK is mainly used for encryption and decryption of sensitive data. Customers can use KMS's automatic CMK generation function or import their own keys to create CMKs. KMS uses FIPS-140-2 certified Hardware Security Modules (HSM) to protect CMKs. CMKs include customer keys and cloud product keys. Customer keys are CMKs created by customers via the console or

No.	Domain	Summary of Controls	Tencent Cloud's Response
			API, for which customers can perform creation, activation, deactivation, rotation, and permission control. Cloud product keys are CMKs automatically created for customers when Tencent Cloud products/services invoke KMS. Customers can query cloud product keys and enable key rotation. <u>CloudAudit</u> service can record operation events related to KMS. Customers can log in to the CloudAudit console to view relevant operation records. To support customers in complying with regulatory requirements, Tencent Cloud has established an internal key management mechanism and formulated relevant standards to regulate key application, generation, storage, usage, transmission, update and destruction. All operations involving the key lifecycle comply with the basic requirements of dual control, strict handover, proper custody and timely update. Rules and systems are established and implemented for segregation of duties, designated responsible persons, strict approval, detailed records and real-name operations. Business key operation logs are retained, and regular operation audits are conducted.
19-2	Management of User Authentication Methods	To prevent the leakage of user authentication methods such as passwords and biometric information, financial companies or electronic financial service providers shall establish and implement management measures, including the issuance, safekeeping, periodic renewal, and handling procedures for authentication failures.	To prevent leakage of user authentication information such as passwords and biometric data, the customer shall adopt measures including the issuance, storage, periodic change of authentication information, and procedures for handling authentication errors. For user biometric authentication and identification, Tencent Cloud provides <u>eKYC</u> to users. eKYC has diverse product advantages and can provide customers with leading, thoughtful, comprehensive and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			secure user facial information verification services, meeting diverse facial authentication needs of customers. eKYC combines Tencent Cloud's years of security experience and leading anti-attack algorithms for facial recognition, which can effectively resist attacks such as static photos, reproduced videos, and 3D masks/head molds, reducing losses caused by identity fraud for customers. In addition, Tencent Cloud ensures the security of cloud products such as eKYC through product testing, regular vulnerability scanning and professional audits. In terms of password management, when customers register user accounts on Tencent Cloud, they set passwords independently through the registration interface. Tencent Cloud provides password policies on the registration interface to assist customers in setting passwords, including requirements for password length and complexity, and prohibits passwords from being the same as the email addresses entered by customers. The Tencent Cloud account registration interface requires customers to enter the set password twice for confirmation to prevent input errors. Additionally, the Tencent Cloud console supports enabling login protection with MFA (Multi-Factor Authentication) on demand, enhancing account security and control measures. Tencent Cloud also provides Cloud Access Management (CAM) to help customers manage access to Tencent Cloud products and resources. Among them, the root account can create sub-accounts and assign identity IDs, credentials and permissions to sub-accounts. Users can modify the password rules of sub-accounts (including password complexity, length, validity period, etc.) and the expiration time of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			single login sessions through the CAM console. To prevent password leakage, Tencent Cloud encrypts passwords with SHA256 Hash and adds Salt, avoiding storing plaintext passwords. In addition, Tencent Cloud has formulated access control management specifications, and sets password policies for employee accounts and cloud customer accounts in accordance with security baselines, including password length, complexity, locking and resetting.

6.1.5 Business Continuity

No.	Domain	Summary of Controls	Tencent Cloud's Response
23	Establishment and operation of emergency measures, etc.	(1) Each financial company and electronic financial business operator shall formulate and observe a plan to ensure business continuity in order to prevent his/her or its business from being suspended in emergency situations, such as system failures, disasters, strikes and terror, including the following: 1. Procedures for response to each situation; 2. Plan for recovery from disasters utilizing backups or the disaster recovery center; 3. Composition and management of an emergency response organization; 4. Conditions and procedures for input on his/her or its behalf, handwork, etc.; 5. Conducting simulated training; 6. Building an emergency liaison	The customer shall formulate and comply with business continuity plans and emergency response manuals and conduct an annual review at a minimum to ensure the effectiveness of business continuity measures. The customer shall provide redundancy or backup for major computer equipment such as central processing units and data storage. The customer shall also establish and operate a disaster recovery center of appropriate scale and staffing at a secure location at a certain distance from the main computing center, and conduct at least one failover drill per year. Tencent Cloud data centers are deployed across Mainland China, Asia Pacific, North America, and Europe, organized into regions and availability zones. Different Tencent Cloud regions are completely isolated from each other, and each region is further divided into multiple isolated availability zones. Currently, Tencent Cloud operates two data centers in South Korea with independent power and network connections, enabling customers to store,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		system with related institutions and enterprises; 7. Scope of and procedures for reporting and external communication. 8. Ensuring and operating emergency support personnel. (3) Each financial company and electronic financial business operator shall examine the effectiveness, appropriateness, etc. of the plan to ensure business continuity under paragraph (1) at least once a year and update and manage it. (4) Any financial company designated by the Financial Services Commission in accordance with the Basic Guidelines for National Emergency Management shall develop and observe an emergency response action manual (hereinafter referred to as "action manual") according to the Finance and Computer Sector Emergency Response Manual of the Financial Services Commission and notify the Financial Services Commission thereof. (5) Each financial company and electronic financial business operator not expressly designated by the Financial Services Commission shall establish and operate an emergency plan to prevent the paralysis of the computer system due to natural disasters, human-induced disasters, technical disasters, electronic trespass, etc. and to	process, and back up data within the country. Customers may independently and flexibly deploy and back up data and systems across different regions or availability zones based on business needs and data security requirements, ensuring business disaster recovery capabilities. To enable customers to quickly respond to and restore critical functions in the event of a cyber security incident, various Tencent Cloud products are designed with high availability to help customers achieve high system or service availability, such as: • <u>Cloud Load Balancer (CLB)</u> provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Cloud Object Storage (COS)</u> provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • <u>Cloud Native Database TDSQL-C:</u> As a next-generation cloud-native relational database independently developed by Tencent Cloud, it adopts a highly available cluster

No.	Domain	Summary of Controls	Tencent Cloud's Response
		ensure prompt recovery from such disasters.	architecture, which can automatically detect faulty nodes and support second-level failover and recovery.
		(6) Action manuals referred to in paragraph (4) or emergency plans referred to in paragraph (5) shall reflect a plan to ensure business continuity under paragraph (1).	• <u>TencentDB for MySQL</u> supports high reliability and availability with robust automatic backup and lossless recovery mechanisms.
		(7) Each financial company and electronic financial business operator shall duplicate the central processing unit, data storage unit, and other main computer equipment or secure reserve devices therefor.	• <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data.
		(8) Financial companies and electronic financial service providers designated under this paragraph shall establish and operate a disaster recovery center equipped with appropriate scale and personnel, located in a safe place at a sufficient distance from the primary computing center, to ensure business continuity and prepare for the paralysis of the computing center due to system failures or natural disasters.	In addition, multiple Tencent Cloud storage and database services offer backup capabilities to support multi-redundant backups, remote disaster recovery, and other requirements. Tencent Cloud provides customers with multi-storage replicas and backup services based on the functions of cloud products or services. Tencent Cloud has designed and implemented a business continuity management framework tailored to its cloud computing environment, built a comprehensive business continuity management system, and formulated business continuity management rules to standardize processes covering business impact analysis, business continuity planning, emergency response and disaster recovery, emergency drills and testing, and crisis management. Tencent Cloud has obtained the ISO/IEC 22301 international certification for Business Continuity Management Systems.
		(9) A financial company referred to in any subparagraph of paragraph (8) shall select core business after analyzing the significance of ensuring business continuity according to each business, and determine the restoration time for each business. In such cases, the restoration time for core business shall be less than three hours and that for core business of insurance companies under the Insurance Business Act, less than 24 hours.	Based on the results of business impact analysis for cloud products and services,
		(10) Any financial company that	Tencent Cloud develops different response

No.	Domain	Summary of Controls	Tencent Cloud's Response
		operates a disaster recovery center under paragraph (8) shall conduct disaster recovery training, at least once a year, assuming that the disaster recovery center actually functions.	strategies and business continuity plans and formulates detailed disaster recovery plans for cloud products and critical processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Tencent Cloud conducts regular drills in strict accordance with requirements to ensure the feasibility of such plans. To ensure continuous availability of customer businesses, Tencent Cloud has implemented redundancy or hot standby mechanisms for hardware devices such as servers, network equipment, and security equipment, ensuring no data loss and recoverable services in the event of hardware failures. Tencent Cloud reviews and updates its business continuity management system annually, and revisits business continuity and disaster recovery plans for relevant products and services based on business impact analysis, making updates as needed. In accordance with internal business continuity management rules, Tencent Cloud also maintains emergency contact lists and designates dedicated personnel to ensure the accuracy and validity of contact information for parties included in these lists.
24	Conducting emergency response exercises	(1) Each financial company or electronic financial business operator shall conduct emergency response training once a year in accordance with the action manual referred to in Article 23 (4) or the emergency plan referred to in	The customer shall conduct an emergency drill annually in accordance with the emergency plan or manual and submit the drill results report to the Financial Services Commission. The customer may adopt the Tencent Cloud Smart Advisor service to assist in

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Article 23 (5) and report the results to the Financial Services Commission. Each financial company or electronic financial business operator may conduct emergency response training along with the disaster recovery training referred to in Article 23 (10). (2) The Financial Services Commission may select financial companies or electronic financial business operators to conduct joint financial sector emergency response training in order to reinforce the capability of the financial sector to respond to emergency situations. (3) In conducting joint emergency response training under paragraph (2), the Financial Services Commission may request the following institutions to provide assistance: 1. The National Intelligence Service (National Cyber Security Center) under Article 17 of the Government Organization Act; 2. The National Police Agency (Cyber Terror Response Center) under Article 12 of the Police Act; 3. The Computer Security Incident Response Team; 4. Other institutions deemed necessary by the Financial Services Commission to secure the effectiveness of emergency response training. (4) A financial company or electronic financial business entity may request cooperation from subsidiary electronic financial	the planning and implementation of business continuity testing. As a cloud governance platform covering vertical applications in multiple ITOM fields, this service relies on the experience of Tencent Cloud's massive operation and maintenance experts to optimize cloud infrastructure through multiple governance measures such as risk inspections and fault drills. Cloud Advisor provides various fault injection scenarios from IaaS to PaaS, as well as drill experience templates for multiple industries, covering multiple typical application scenarios such as cross-AZ disaster recovery, helping customers quickly and efficiently reuse mature solutions according to their own business needs and improve system availability. To assist customers in complying with regulatory requirements, 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 classic disaster recovery scenarios, including attack and defense confrontations and large-scale faults, to comprehensively check the system's disaster recovery capabilities, response speed and recovery capabilities. After the drill, the relevant departments organize and compile a drill report, rectify according to the improvement measures, and file and store the report. Tencent Cloud may also provide relevant technical support to customers for their security drills when appropriate.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		business operators ⁶ to fulfill the obligations specified in Paragraphs (1) and (2).	
25	Performance Management of Information Processing System	Each financial company and electronic financial business operator shall regularly conduct an analysis, etc. of the status of use and development of the information processing system in order to prevent system failures and optimize system performance.	The customer shall regularly analyze the usage status and trends of information processing systems to prevent failures and optimize system performance. Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. The customer may use Tencent Cloud Observability Platform (TCOP) to conduct real-time monitoring, analysis and alerting on cloud products/resources. TCOP can collect and display various monitoring indicators self-reported by Tencent Cloud products and customer-customized monitoring indicators through visual charts, helping the customer grasp the operational status and performance of cloud products in real time. Tencent Cloud also provides customers with a one-stop security management platform, Cloud Security Center (CSC) which can collect threat alerts and logs from Cloud Firewall and Web Application Firewall, and conduct automated analysis and investigation on the data by leveraging Tencent Cloud threat intelligence and its own security knowledge

⁶ an entity that provides auxiliary services for electronic financial transactions or acts as an agent for some of such transactions on behalf of financial companies or electronic financial service providers, or an operator of a payment intermediary system, as designated by the Financial Services Commission (hereinafter referred to as the "Financial Services Commission") in accordance with Article 3 of the 「Act on the Establishment of the Financial Services Commission, etc.」.

No.	Domain	Summary of Controls	Tencent Cloud's Response
34	Compliances in Electronic Financial Transactions	Each financial company and electronic financial business operator shall comply with the following with respect to electronic financial transactions: 1. Encrypted communications shall be used for electronic financial transactions, except telephones or other means of communications to which encryption itself cannot be applied in view of the nature of a means of transactions (Provided, That this shall not apply where private lines are used and self-examinations of security levels thereof has been conducted pursuant to Article 36)	base, providing customers with centralized threat detection, investigation and response capabilities.
			The customer shall apply communication encryption to electronic financial transactions, unless encryption is not feasible due to the inherent nature of transaction methods such as telephone, or in other cases exempted in accordance with regulations. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Tencent Cloud has established a baseline for data security management, clearly mandating the use of secure data transmission protocols for sensitive data transfer while prohibiting the use of insecure transmission protocols. This ensures the security and integrity of customers' sensitive business data during transmission. Customers can further enhance data transmission security using the following services: • <u>Direct Connect (DC)</u>: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • <u>VPN Connection</u>: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission.

6.1.6 Vulnerability Analysis and Incident Response

No.	Domain	Summary of Controls	Tencent Cloud's Response
37-2	Cycle, Content, etc. of Analysis and Evaluation of Weak Points of Electronic Network for Financial Transactions	(1) Each financial company or electronic financial business operator, the total assets of which are at least two trillion won and the number of regular employees (based on persons from the payment to whom a person obligated to withhold tax under the Income Tax Act collects earned income tax; hereinafter the same shall apply) of which is at least 300, shall conduct analysis and evaluation of weak points in an electronic network for financial transactions at least once a year (for the homepage, at least once a half year). (2) Each financial company and electronic financial business operator shall organize an in-house task force comprised of at least five persons including the chief information security officer (where the chief information security officer does not exist, the chief executive officer shall designate him/her) for analysis and evaluation of weak points in an electronic network for financial transactions, and at least 30 percent of the constituent members shall be qualified for high quality technical personnel prescribed by the standards for designation of specialized information security service enterprises prescribed in Article 8 of the Enforcement Rule of the Act on the Promotion of Information Security Industry: Provided, That where it entrusts	The customer shall conduct vulnerability analysis and assessment of electronic financial transaction networks at least once a year (and at least once every six months for the main website). The assessment may be performed by an internal specialized team or an external evaluation organization. The customer shall also formulate and implement a remediation plan based on the assessment results to eliminate vulnerabilities or implement remedial/critical measures. The customer may use the Vulnerability Scan Service (VSS) to detect enterprise network assets and identify risks. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation advice to reduce security risks. VSS can integrate with other Tencent Cloud products such as Host Security and Web Application Firewall to achieve a closed-loop process from risk monitoring to risk mitigation. Tencent Cloud has also established internal threat and vulnerability management procedures to promptly identify and take measures to address threats and vulnerabilities facing information systems. Tencent Cloud regularly generates scan tasks through a vulnerability scanning system to conduct vulnerability scans on assets in the cloud environment, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		such analysis and evaluation to an institution specialized in evaluation under Article 37-3 (1), it may choose not to organize an in-house task force. (3) A person, other than a financial company or electronic financial business operator under paragraph (1), shall conduct analysis and evaluation of weak points in an electronic network for financial transactions at least once a year (for the homepage, at least once a half year), but may choose not to organize an in-house task force. In such cases, details of analysis and evaluation of weak points shall be prescribed by the Governor of the Financial Supervisory Service. (4) Each financial company and electronic financial business operator may conduct evaluations by dividing facilities subject to evaluation and periods of evaluation. (5) Each financial company and electronic financial business operator shall formulate and execute an implementation plan according to analysis and evaluation of weak points, and comply with the following matters: 1. Eliminating weak points as a result of analysis and evaluation of weak points or taking actions corresponding thereto; 2. Where it is impracticable to eliminate weak points or take actions corresponding thereto, approval shall be obtained from the	analyzes, classifies, and repairs the identified vulnerabilities. If the assessment finds that vulnerabilities may impact customer businesses, 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 vulnerability descriptions, scope and degree of impact, control measures taken by Tencent Cloud, remediation suggestions and specific operation guidelines for customers. Tencent Cloud has also established an external vulnerability feedback platform and launched a "Vulnerability Reward Program" to invite security experts in the industry to help Tencent Cloud discover system security vulnerabilities and risks from a hacker perspective, fix security issues in a timely manner, and maintain the ecological security of Tencent Cloud.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		chief executive officer; 3. Results of the execution of an implementation plan shall be reported to the chief executive officer. (6) A financial company or electronic financial business entity may request cooperation from subsidiary electronic financial business operators to fulfill the obligations specified in Paragraphs (1) and (3).	
37-4	Methods for Reporting Violations and Incidents	Financial companies and electronic financial service providers must immediately report to the Financial Services Commission by recording the incident details and its impact on the <Annex 7 Form> upon discovering a violation incident under Article 21-5 of the law, and must not exceed 24 hours from the time of discovery without justifiable reasons.	The customer shall, upon learning of an accident caused by electronic infringement (such as disrupting and paralyzing the electronic financial infrastructure), report the details of the accident and its impact to the Financial Services Commission within 24 hours in accordance with the prescribed form. To assist the customer in effectively fulfilling the obligation of communication and notification, Tencent Cloud has formulated the Information Security Incident Management Specification and established relevant procedures for information security incident response, incident escalation, and incident notification to promptly warn or notify internal personnel of the company, customers and other relevant parties that may or have been affected by the accident, ensuring that all parties can conduct communication and coordination in an orderly, timely and efficient manner. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results of the information security incident through appropriate methods according to the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			impact scope and degree of the information security incident, and provide corresponding technical support to assist the customer in taking remedial measures to minimize losses.
37-5	IT Industry and Electronic Financial Incident Reporting	(1) Financial companies and electronic financial service providers shall comply with the following provisions regarding incidents in the information technology industry and electronic finance: 1. Establish and operate procedures including classification of incident types, handling steps, response methods, methods for assessing the impact extent and severity, etc. 2. In the event of an incident defined by the Financial Supervisory Service, promptly report it to the Financial Supervisory Service. (2) Financial companies and electronic financial service providers shall take necessary measures, such as disciplinary action, in accordance with prescribed procedures against any person who intentionally delays or conceals the incident report under Paragraph (1) Subparagraph 2. (3) The Financial Supervisory Service shall immediately report the content received under Paragraph (1) Subparagraph 2 to the Financial Services Commission. (4) Details regarding incident reporting under Paragraph (1)	The customer shall establish and implement procedures related to incident response, classification, assessment and handling, and immediately report to the Financial Supervisory Service when an accident as defined by the Financial Supervisory Service occurs. Tencent Cloud has formulated information security incident management specifications for incident response and handling, established information security reporting, response and handling mechanisms and relevant procedures, and clarified the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud records security incidents using an internal security operations system. For detected and identified security incidents, Tencent Cloud analyzes and classifies the incidents based on factors such as the nature of the incident, data sensitivity and scope of impact, and promptly notifies the responsible personnel to follow up and handle the incidents. Relying on its 7×24-hour security operation system, Tencent Cloud Security Team focuses on core scenarios such as vulnerability monitoring, intrusion traceability and attack blocking, responds to security alerts in real time, and quickly completes attack traceability and formulation of emergency response plans, effectively curbing the spread of security incidents. For security incidents that may affect customers, Tencent Cloud will notify customers of the handling and analysis

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Subparagraph 2, including the scope of reportable incidents, procedures, methods, etc., shall be stipulated by the Financial Supervisory Service.	results of the information security incident through appropriate methods after internal review based on the scope and degree of impact of the information security incident.
37-6	Designation and Scope, etc. of Work of Computer Security Incident Response Teams	(1) Computer security incident response teams for responding to computer security incidents shall be as follows: 1. The Financial Security Institute; 3. A person designated by the Chairperson of the Financial Services Commission. (5) Each financial company and electronic financial business operator shall formulate and execute a computer security incident response and recovery training plan at least once a year to ensure the ability to respond to computer security incidents; and shall submit the plan and the results thereof to the head of the relevant computer security incident response team: Provided, That this shall not apply to the following financial companies: 1. Credit unions among financial companies referred to in subparagraph 3 (a) of Article 2 of the Act; 2. Financial companies referred to in subparagraph 3 (c) and (d) of Article 2 of the Act; 3. Cooperatives referred to in subparagraphs 4 through 6 of Article 2 of the Enforcement Decree; 4. Financial companies meeting requirements referred to in Article	Customers shall formulate and implement an incident response and recovery drill plan at least once a year and submit the plan and results to the relevant incident response authority (e.g., the Financial Supervisory Service). Customers shall also cooperate with the authority in inspections on incident response, recovery and training results, and implement improvements in accordance with guidance. Customers may use the Tencent Cloud Smart Advisor (TSA) service to assist in the planning and implementation of incident response and recovery drills. As a cloud governance platform for vertical applications in multiple ITOM fields, it relies on Tencent Cloud's massive experience of operation and maintenance experts to optimize cloud infrastructure through multiple governance measures such as risk inspection and fault drills. Cloud Advisor can provide various fault injection scenarios from IaaS to PaaS, as well as drill experience templates for multiple industries, covering multiple typical application scenarios such as cross-AZ disaster recovery, helping customers quickly and efficiently reuse mature solutions according to their own business needs and improve system availability. To assist customers in complying with regulatory requirements, Tencent Cloud conducts regular emergency response and disaster recovery drills and tests. Tencent Cloud formulates drill plans based on business continuity plans, conducts drill risk assessments, formulates corresponding

No.	Domain	Summary of Controls	Tencent Cloud's Response
		5 (2) of the Enforcement Decree.	safeguard measures, and avoids negative impacts on services caused by drills. Tencent Cloud's disaster recovery drills are often conducted by simulating real classic disaster recovery scenarios, including attack and defense confrontations and large-scale faults, to comprehensively check the system's disaster recovery capability, response speed and recovery capability. After the drill, the relevant departments organize the preparation of a drill report, rectify according to improvement measures, and file and retain the report. Tencent Cloud may also provide relevant technical support for customers' security drills where appropriate.

6.2 Licensing, Registration, and Operations of Electronic Financial Affairs

No.	Domain	Summary of Controls	Tencent Cloud's Response
50	Detailed Requirements for Personnel and Physical Facilities	(1) A person who intends to obtain a license or apply for registration under Articles 28 and 29 of the Act shall meet all of the following requirements related to personnel and physical facilities: 1. Securing not less than five executives or employees having experience in computer business for at least two years at the time of the application, or being able to secure such executives or employees at the time of the license or registration; 2. Being equipped with the computer equipment necessary for the smooth operation of the electronic financial business; 3. Having the backup devices to	To obtain the license, customers shall ensure that aspects such as staffing, computer equipment, backup mechanisms, information security and monitoring-related systems, and computer room security comply with regulatory requirements. For the monitoring and analysis of information assets, The customer may use Tencent Cloud Observability Platform (TCOP) to conduct real-time monitoring, analysis and alerting on cloud products/resources. TCOP can collect and display various monitoring indicators self-reported by Tencent Cloud products and customer-customized monitoring indicators through visual charts, helping the customer grasp the operational status and performance of cloud products in real time. Tencent Cloud also provides customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
		prevent the loss of computer data from any computer system failure;	with a one-stop security management platform, Cloud Security Center (CSC)
		4. Having various programs essential for the smooth operation of electronic financial businesses;	which can collect threat alerts and logs from Cloud Firewall and Web Application Firewall, and conduct automated analysis and investigation on the data by leveraging
		5. Developing an information processing system management plan appropriate to protect computer data, and establishing a monitoring and operating system, such as an information protection system ⁷ ;	Tencent Cloud threat intelligence and its own security knowledge base, providing customers with centralized threat detection, investigation and response capabilities.
		6. Ensuring the safety of the structure, interior materials, facilities, etc. of the IT room and developing a proper security plan.	In terms of disaster recovery and backup , Tencent Cloud has designed and implemented a business continuity management framework tailored to its cloud computing environment, built a comprehensive business continuity management system. Tencent Cloud has obtained the ISO/IEC 22301 international certification for Business Continuity Management Systems.
			Tencent Cloud data centers are deployed across Mainland China, Asia Pacific, North America, and Europe, organized into regions and availability zones. Different Tencent Cloud regions are completely isolated from each other, and each region is further divided into multiple isolated availability zones. Customers may independently and flexibly deploy and back up data and systems across different regions or availability zones based on business needs and data security requirements, ensuring business disaster recovery capabilities.
			To ensure the continuous availability of customers' businesses, Tencent Cloud requires cloud products to adopt a redundancy mechanism with multiple data centers in a single region. Tencent Cloud

⁷ "information protection system" means any and all equipment and programs to prevent information in any information processing system from being divulged, falsified, altered, or otherwise compromised or to protect any information processing system from the interruption of its normal service.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			also sets up redundancy or hot standby mechanisms for hardware devices such as servers, network equipment, and security equipment to ensure no data loss and recoverable businesses in case of hardware failures. Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customer needs, such as: • <u>Cloud Object Storage (COS):</u> Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS):</u> Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS):</u> Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C:</u> Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL:</u> Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB:</u> Offers automated backup and lossless recovery mechanisms, supporting

No.	Domain	Summary of Controls	Tencent Cloud's Response
			multi-node backups and retention of multiple days of backup data for disaster recovery scenarios. In terms of physical environment security, Tencent Cloud has formulated physical security management systems to standardize operational security, identify risks in a timely manner, and strengthen physical security management. Tencent Cloud's data centers worldwide are selected, constructed, or leased in accordance with relevant international standards and local security requirements. Tencent Cloud has deployed two leased data centers in South Korea. To ensure the resilience and security of data centers, Tencent Cloud has built a strict management system throughout the entire process from data supplier access, protocol constraints to continuous supervision. Tencent Cloud conducts regular internal and external audits every year and conducts on-site inspections of operator data centers to ensure that they meet the information security requirements stipulated by Tencent Cloud. Tencent Cloud requires operators to install smoke detectors, lightning protection and grounding devices, fire alarms and water sprinkler systems, power supply systems, shunt circuit systems, fresh air systems, air conditioning systems, and temperature monitoring devices in data centers, and arrange personnel to provide maintenance around the clock to support the rapid resolution of equipment failures. Tencent Cloud also requires data center operators to formulate physical security emergency plans and regularly organize drills for data center staff. For physical security and monitoring,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud requires security personnel at data center operators to conduct inspections of each computer room and equipment in strict accordance with inspection lists and plans, sign and record the inspection time at each inspection point and immediately activate the data center emergency response process when infrastructure failures or security incidents are found. Tencent Cloud also requires operators to equip data centers with a 7x24-hour non-blind spot video monitoring and alarm system manned by a security room and ensure the secure retention of monitoring records for a sufficient period of time.

6.3 Supervision of Electronic Financial Affairs

No.	Domain	Summary of Controls	Tencent Cloud's Response
60	Standards for Outsourcing	(1) If a financial company or electronic financial business operator outsources its or his/her electronic financial transactions, it or he/she shall comply with the following: 1. Separately installing and operating a workplace and computer facilities used for the development of the information processing system based on outsourcing, etc. from those used for internal business; 2. Prohibiting the de-encryption of encrypted information between the financial company and users and the alteration of material data, such as the ledger; 3. Prohibiting the storage or disclosure without permission of	When a customer outsources electronic financial transaction services, it shall comply with a series of regulations, including separating the business premises and computer equipment related to the development of outsourced information processing systems from internal businesses, adopting security measures such as anti-counterfeiting and information leakage prevention, connecting with electronic financial service providers via dedicated lines, formulating backup and emergency countermeasures, continuously evaluating electronic financial service providers, and prohibiting the outsourced party from subcontracting without authorization. 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 users' financial information, such as their account numbers and passwords;	<u>Service, Service Level Agreement (SLA), and 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.
		4. Establishing security measures against falsification and alteration of access media, hacking, divulgence of personal information, etc.;	
		5. Using a dedicated line (including virtual dedicated lines of security level equivalent to that of dedicated lines) for connecting the financial company to its subsidiary electronic financial business operator;	Regarding subcontracting , the agreement clearly stipulates clauses such as prior consent for subcontracting, notice before adding or replacing subcontractors, and data protection obligations. Without the customer's prior consent, Tencent Cloud will not subcontract any processing operations it performs on behalf of the customer in accordance with the contract/agreement. For any anticipated changes involving the addition or replacement of subcontractors, Tencent Cloud will notify the customer via channels such as email.
		6. Establishing emergency plans against suspension of service, such as information processing system failures;	
		7. Complying with the security control schemes prescribed by the Governor of the Financial Supervisory Service for each stage, including a tender or contract for outsourcing, etc., performance of the contract, completion of performance of the contract, etc.;	In terms of subcontractor management , Tencent Cloud has established a comprehensive supply chain security management system, effectively controlling suppliers through strict supplier security assessment and admission, regular monitoring and evaluation, and clear outsourcing service agreements, ensuring that subcontracting will not affect Tencent Cloud's ability to provide relevant services to customers or the confidentiality and integrity of the customer information processing process.
		8. Establishing backup plans to ensure business continuance, such as preservation of backup data for important computer data and securing of backup equipment;	In terms of protecting customer data , customer data is classified as high-security-
		9. Establishing and implementing internal control policies to minimize the vulnerabilities of information management and maintain security, which are subject to control by the organization referred to in Article 8 (1) 2;	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		10. Evaluating the financial soundness of a subsidiary electronic financial business operator at least once a year for preparing for bankruptcy that may be caused by his/her financial aggravation, and constantly monitoring his/her major management activities; 11. Evaluating the quality of service provided by a subsidiary electronic financial business operator at least once a year; 12. Prohibiting a subsidiary electronic financial business operator from subcontracting its outsourcing, etc. or changing a subcontract enterprise without prior consent, and, when giving prior consent to a subcontract, requiring him/her to specify the matters listed in subparagraph 7 in the subcontract; 13. Conducting a preliminary background check on the personnel performing the work (in this case, it can be replaced by obtaining a fidelity bond) or obtaining a letter of guarantee from the representative, establishing a management plan for the personnel performing the work, including matters related to the handover of personnel when personnel changes, etc.; 14. Conducting self-examinations of security levels and regular (daily, for important matters determined by the Governor of the Financial Supervisory Service) security checks, associated with	level data within Tencent Cloud, and the customer has exclusive ownership and control over its own data content. Unless necessary for providing services or troubleshooting, and with the customer's explicit authorization or in cases of investigations into criminal cases by national or local government departments in accordance with national laws and regulations, Tencent Cloud employees will never proactively access any customer data. Tencent Cloud protects customer data by implementing access control and permission management, signing non-disclosure agreements with employees, deploying Data Loss Prevention (DLP) tools, and other measures. To assist customers in data storage protection, many Tencent Cloud storage and database products support data encryption functions using secure high-strength encryption algorithms, and achieve full lifecycle key management by integrating the Key Management Service (KMS) to ensure data confidentiality. For transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling

No.	Domain	Summary of Controls	Tencent Cloud's Response
		outsourcing, etc.	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.
		(2) Each financial company and electronic financial business operator shall report the outcomes of evaluation under paragraph (1) 10 and 11 to the Governor of the Financial Supervisory Service.	To ensure the continuous and stable availability of customers' businesses, Tencent Cloud builds or leases data centers in multiple regions worldwide in accordance with relevant international standards and local security requirements, providing customers with multi-region and multi-availability zone options to meet business disaster recovery requirements and service levels. Various cloud products/services provided by Tencent Cloud, including computing services, network services, storage services, database services, container and middleware services, and security services, feature high availability and have corresponding disaster recovery plans. Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. To assist customers in implementing backup strategies, Tencent Cloud provides multi-storage replica and backup services to customers based on the functions of cloud products or services, and assumes responsibility for the provided data backup

No.	Domain	Summary of Controls	Tencent Cloud's Response
			services in accordance with the agreements in the product service level agreements (SLAs). Various cloud products/services offered by Tencent Cloud, including computing services, network services, storage services, database services, container and middleware services, support customers in configuring backup policies for their own systems and data to meet various backup needs. To support customers' outsourcing evaluation and inspection requirements, Tencent Cloud can assign dedicated personnel to assist and actively respond to audit or review activities initiated by customers. 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 organizations, independent auditors, regulatory authorities, company shareholders and other relevant stakeholders by providing assurance-type System and Organization Controls (SOC) reports. Regarding the management of business execution personnel, Tencent Cloud has established comprehensive internal human resource management standards and procedures to ensure that recruitment and personnel assignments align with job requirements. During the recruitment process, Tencent Cloud conducts thorough reviews of potential candidates, assessing their integrity, professional qualifications, past records, and compliance risks to ensure they meet both the position requirements and the company's security management standards.

6.4 Standards for Evaluating the Soundness and Safety of Cloud Computing Service Providers

Appendix 2-2 Standards for Evaluating the Soundness and Safety of Cloud Computing Service Providers include the standards for financial companies and electronic financial service providers to evaluate the security of cloud service providers pursuant to subparagraph 2 of paragraph (1) of Article 14-2, which are divided into “Required” standards and “Alternative” standards.

Under these Regulations, the evaluation of “Alternative” items may be omitted if the relevant business is classified as a non-material business pursuant to subparagraph 1 of paragraph (1) of Article 14-2, or if it is confirmed that the cloud service provider continuously holds security certifications related to cloud services in South Korea and abroad.

Tencent Cloud has obtained the Korea Information Security Management System (K-ISMS) certification and undergoes regular audits by KISA annually. For more details on Tencent Cloud's certification qualifications, please refer to Chapter 2 "[Tencent Cloud Security and Privacy Compliance](#)" of this guide.

This chapter describes how Tencent Cloud, as a cloud service provider, complies with the relevant standards and requirements.

6.4.1 Information Protection and Law Observance

No.	Domain	Summary of Controls	Tencent Cloud's Response
1.1	Information Protection	1.1.1.[Alternative] Does the provider establish and enforce information protection policies and guidelines organization-wide?	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
	Strategy	1.1.2. [Alternative] Does the provider have procedures in place to periodically review, evaluate, amend, and supplement its information protection policies?	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. In terms of regular reviews and assessments, the Tencent Cloud Security Team conducts internal security audits at least once a year to ensure compliance with the provisions and requirements of relevant laws and regulations as well as security management standards. Tencent Cloud also regularly accepts professional audits from independent third parties and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulators, company shareholders and other relevant stakeholders by providing attestation-based System and Organization Controls (SOC) reports. Specifically for South Korea, Tencent Cloud has obtained the Korea Information Security Management System (K-ISMS) certification.
1.2	Information Protection Organization	1.2.1 [Alternative] Has the provider established a dedicated information protection organization to efficiently ensure security and protect users? 1.2.2 [Alternative] Are roles and responsibilities for information security and information assets, assigned to relevant employees, clearly defined, including those related to users' information protection?	In terms of the organizational structure for information security management, Tencent Cloud has established organizational structures related to cloud security and information security, clarifying security functional roles and related responsibilities at different levels, and defining working mechanisms such as information security audits and information security risk assessments. Tencent has set up a Security Technology Committee and professional security teams in different functions and fields, and has established a sound human resource management system and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			procedures internally to ensure that personnel are recruited and arranged in accordance with job requirements. Tencent Cloud brings together a senior expert service team in the industry, committed to providing customers with safe, reliable, professional and compliant products and services.
			Tencent Cloud strictly abides by the laws and regulations of the jurisdictions where it operates its business, identifies and adopts advanced international and industry security standards, and has established security and compliance-related procedures to improve Tencent Cloud's security and compliance capabilities and build a cloud service worthy of customer trust.
1.3	Law Observance	1.3.1 [Required] Does the provider have systems in place to assist users in meeting legal and regulatory obligations?	To date, Tencent Cloud has obtained a number of security and privacy compliance certifications or qualifications through third-party independent audits or assessments, which prove that Tencent Cloud's security management and privacy protection construction meet the relevant certification standards or industry best practices. For more information on Tencent Cloud's compliance, please refer to the Tencent Cloud Compliance page. If you need any relevant compliance certificates or reports, please apply and download them through the Tencent Cloud Compliance Document Center .
1.4	Security Audit	1.4.1 [Required] Does the provider define the subjects of access log recording, maintain and monitor security audit logs in an identifiable format to ensure service control and incident traceability, and protect them from unauthorized access and modification?	Tencent Cloud provides CloudAudit for supervising Tencent Cloud account activities, compliance checks, operational reviews, and risk assessments. With CloudAudit, customers can capture a comprehensive historical record of changes that occurred within their Tencent Cloud accounts during specific periods, enabling them to identify and resolve security and operational issues. Cloud Log Service

No.	Domain	Summary of Controls	Tencent Cloud's Response
			(CLS), a one-stop log service platform to assist customers in solving problems such as business operation, security monitoring, log auditing, and log analysis. In addition, customers can use Elasticsearch Service (ES) to aggregate and transmit real-time logs of other cloud products such as cloud servers and containers, or stock and incremental business data of services to the Tencent Cloud ES cluster for distributed storage and query analysis of data. Tencent Cloud internally has established log collection and management specifications and mechanisms to control the recording, extraction, analysis, auditing, and other aspects of log data such as login logs, operation logs, and event logs, so as to detect and prevent abnormal system activities and risks. At the same time, Tencent Cloud has set detailed operation and maintenance security "red lines" and established a perfect rule library based on years of accumulated experience in abnormal behavior monitoring, creating a reliable operation and maintenance security automated auditing tool that can timely identify abnormal behaviors and automatically trigger real-time alarms.

6.4.2 Personnel Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.1	Internal Personnel Security	2.1.1 [Alternative] Are all employees involved in the operation, development, and security of cloud services designated as key personnel and managed appropriately? 2.1.2 [Alternative] Have duty separation standards been established and implemented to reduce potential internal threats that may arise from intentional act	Tencent Cloud has established an organizational structure related to cloud security and information security. Based on principles such as separation of duties, it clarifies the roles and related responsibilities of security functions at different levels, and defines working mechanisms such as information security audit and information security risk assessment. Tencent has set up a security technology committee and professional

No.	Domain	Summary of Controls	Tencent Cloud's Response
		by employees, such as abuse of authority? 2.1.3[Alternative] Is it ensured that information assets are promptly returned, and access rights are updated or revoked without delay when personnel changes occur within the organization?	security teams with different functions and fields, and has established a sound set of human resource management standards and procedures internally, including entry procedures, employment period procedures, and exit procedures, to ensure that personnel are recruited and arranged in accordance with the job requirements. Before employment, applicants will undergo an interview, and Tencent Cloud assesses whether they have the abilities required for the position. In accordance with applicable laws and the position level, the human resources department conducts a background check on candidates before employment. The background check includes verifying past work experience, criminal record check, and educational background verification. The results of the background check are recorded in Tencent Cloud's human resource management system. After accepting employment, all internal employees are required to sign an employment agreement and a non-disclosure agreement. The employment agreement clarifies Tencent Cloud's existing security policies and the information security and personal information protection responsibilities that employees or third-party personnel should perform. The non-disclosure agreement includes the confidentiality obligations and responsibilities of the signatory, as well as possible penalties for breaching the confidentiality clauses. During their employment, Tencent Cloud has established a series of information security training and learning mechanisms to educate employees on information security policies, procedures, and guidelines. Employees regularly participate in

No.	Domain	Summary of Controls	Tencent Cloud's Response
			information security awareness training.
			Tencent Cloud's exit procedures include processes such as timely terminating user accounts and permissions and recovering company assets. All physical assets of Tencent Cloud are assigned to designated responsible persons and registered through Tencent Cloud's dedicated internal asset tracking system. Tencent Cloud conducts asset inventory regularly to confirm the actual existence of assets and records the inventory results.
2.2	External Personnel Security	2.2.1 [Alternative] Does the provider periodically inspect outside workers in respect of their compliance with security requirements and take appropriate measures in response to any violation or security incidents?	For the management of outsourced employees, Tencent Cloud has established a comprehensive supply chain security management system to supervise and manage the activities of supplier personnel, and conduct regular evaluations to ensure that the activities of suppliers and their related personnel comply with Tencent Cloud's corresponding rules and regulations. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.

6.4.3 Risk Assessment and Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.1	Asset Identification and Classification	3.1.1 [Alternative] Does the provider establish asset classification standards for information assets (e.g.,	In terms of information asset management, Tencent Cloud has formulated information asset management specifications and a full life-cycle management process, classifying

No.	Domain	Summary of Controls	Tencent Cloud's Response
		information system, protection system, data) used in cloud computing services, and maintain a list of the identified assets?	and protecting 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 retirement and replacement, etc., to ensure the stable operation of the underlying cloud platform system and provide reliable support for business systems.
3.2	Asset Change Management	3.2.1 [Alternative] Does the provider establish and implement control procedures to ensure uninterrupted cloud computing services during system integration, conversion, or redevelopment?	Tencent Cloud has established a set of standards for product and configuration change management, clarifying each step in the change process and relevant responsible persons to ensure that changes undergo appropriate approval and testing before implementation. At the same time, Tencent Cloud defines a management process for emergency changes, which can only be carried out after obtaining appropriate approval. All types of procedural changes, including changes to applications and configuration files, operating systems, and databases, require a business impact analysis before going live, a rollback plan for the change must be formulated, and approval by relevant responsible persons is necessary. Tencent Cloud's change release system mandates that change operations can only be performed by authorized personnel, and logs related to changes are retained and regularly reviewed. After a change is released, Tencent Cloud operations team verifies, monitors, and records the results in the production environment. In addition, Tencent Cloud classifies impact levels based on attributes such as the importance/urgency of operation and maintenance requests and the scope of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			changes. For change requests that may affect products, infrastructure, and network configurations in the external environment, Tencent Cloud will notify customers through announcements, emails, the Tencent Cloud console, and/or other appropriate channels.
3.3	Risk Management	3.3.1 [Alternative] Does the provider periodically inspect vulnerabilities in core assets and services, and take appropriate measures to mitigate identified risks?	Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform. Tencent Cloud uses a vulnerability scanning system to regularly scan for security vulnerabilities in the cloud environment. The scanning scope covers the virtualization layer, system layer, and application layer. Upon completion of the 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.

6.4.4 Service Supply Chain Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.1	Supply Chain Management Policy	4.1.1 [Alternative] Does the provider establish and implement management policies that define security requirements related to the supply chain?	Tencent Cloud has established a sound supply chain security management system. Through strict supplier security assessment and admission, regular monitoring and evaluation, and clear outsourcing service agreements, it effectively manages suppliers to ensure that subcontracting will not affect Tencent Cloud's ability to provide relevant services to customers, as well as the confidentiality and integrity of the customer information processing process.
4.2	Supply Chain Change Management	4.2.1 [Alternative] Does the provider regularly monitor and review records and reports generated throughout the supply chain?	Tencent Cloud has established a regular monitoring and evaluation mechanism. It conducts comprehensive assessments of suppliers' technical capabilities, service response efficiency, and risk management and control effects on a regular basis to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			ensure that core service capabilities provided by Tencent Cloud to customers will not be affected due to the risks or deficiencies in supplier management. In strict accordance with the Service Level Agreements (SLAs) signed by both parties, Tencent Cloud requires suppliers to submit SLA performance fulfillment reports as agreed cycles. These reports must cover core contents such as major incident handling records, key performance indicator achievements, and maintenance work summaries during the service cycle. Tencent Cloud conducts regular performance evaluations on suppliers, and the results of such evaluations serve as an important basis for future supplier cooperation.

6.4.5 Task Continuity Plan and Failure Recovery

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.1	Failure Response	5.1.1 [Alternative] Does the provider establish and implement a task continuity plan to ensure that cloud services are not suspended?	Tencent Cloud has designed and implemented a business continuity management framework tailored to its cloud computing environment, built a comprehensive business continuity management system, and formulated business continuity management rules to standardize processes covering business impact analysis, business continuity planning, emergency response and disaster recovery, emergency drills and testing, and crisis management. Tencent Cloud has obtained the ISO/IEC 22301 international certification for Business Continuity Management Systems. Tencent Cloud data centers are distributed across multiple regions worldwide, consisting of regions and availability zones, and covering Mainland China, Asia Pacific, North America, and Europe. Currently, Tencent Cloud has deployed two leased

No.	Domain	Summary of Controls	Tencent Cloud's Response
			data centers in South Korea. Customers can independently and flexibly deploy data and systems across different regions or availability zones according to business development needs and data security requirements to ensure business disaster recovery capabilities. In addition, Various cloud products and services provided by Tencent Cloud, including computing services, network services, storage services, database services, container and middleware services, feature high availability, such as: • <u>Cloud Load Balancer (CLB)</u> provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Cloud Object Storage (COS)</u> provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • <u>Cloud Native Database TDSQL-C:</u> As a next-generation cloud-native relational database independently developed by Tencent Cloud, it adopts a highly available cluster

No.	Domain	Summary of Controls	Tencent Cloud's Response
			architecture, which can automatically detect faulty nodes and support second-level failover and recovery. • <u>TencentDB for MySQL</u> supports high reliability and availability with robust automatic backup and lossless recovery mechanisms. • <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data.
	5.1.2 [Required] In the event of a cloud service outage or damage, does the provider record such failure according to the failure reporting procedure and provide relevant information to help users understand the status?		Tencent Cloud has formulated information security incident management specifications for incident response and handling, established information security reporting, response and handling mechanisms and relevant procedures, and clarified the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud records security incidents using an internal security operations system. For detected and identified security incidents, Tencent Cloud analyzes and classifies the incidents based on factors such as the nature of the incident, data sensitivity and scope of impact, and promptly notifies the responsible personnel to follow up and handle the incidents. For security incidents that may affect customers, Tencent Cloud will notify customers of the handling and analysis results of the information security incident through appropriate methods after internal review based on the scope and degree of impact of the information security incident. and provide corresponding technical support to assist customers in taking

No.	Domain	Summary of Controls	Tencent Cloud's Response
			remedial measures to minimize losses.
			In terms of the collection and management of incident evidence/information, Tencent Cloud has clearly formulated relevant standards for the collection of security incident evidence internally. During the acceptance, investigation and evaluation, handling, and tracking of information security incidents, relevant responsible departments will maintain records related to the accepted information security incidents and ensure the integrity and confidentiality of the records. Tencent Cloud will, based on customers' needs and on the basis of evaluating rationality and feasibility, provide effective support for customers' digital forensics and post-incident security incident investigation and analysis.
			To ensure the continuous availability of cloud services, Tencent Cloud conducts a business impact analysis on cloud products and services, defines the recovery time objective (RTO) and recovery point objective (RPO) for each business, and formulates corresponding response strategies and business continuity plans based on the results of the business impact analysis. Detailed disaster recovery and recovery plans are developed for cloud products and key 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.
		5.1.3 [Alternative] In the event of a cloud service disruption or damage, can the provider address and recover from failures within a target recovery time?	Tencent Cloud also regularly conducts business continuity drills and tests for cloud products in accordance with its business

No.	Domain	Summary of Controls	Tencent Cloud's Response
			continuity plans to ensure the feasibility of the plans. Tencent Cloud has further clarified processes for the monitoring and reporting of emergencies, emergency response, disaster recovery, and crisis management, striving to minimize the adverse impacts of emergencies in the shortest possible time. It uses an emergency alert system for event reporting, analysis and incident classification, and carries out disposal or recovery work based on the recovery time requirements and response strategies corresponding to the incident level, so as to avoid and mitigate losses caused by service interruptions to asset security and business operations to the greatest extent.
5.2	Service Availability	5.2.1 [Required] Does the provider ensure redundancy in information processing facilities, such as virtualization servers and equipment, and develop and maintain a backup system to prevent service suspension due to facility failures?	Tencent Cloud data centers are distributed across multiple regions globally, consisting of regions and availability zones, covering mainland China, the Asia-Pacific region, North America, and Europe. Currently, Tencent Cloud has deployed two leased data centers in South Korea. Customers can flexibly deploy data and systems across different regions or availability zones according to their business development needs and data security requirements, and adopt different business continuity models to meet business disaster recovery requirements. In addition, Tencent Cloud has set up redundancy or hot standby mechanisms for hardware devices such as servers, network equipment, and security equipment to ensure no data loss and business recoverability in the event of hardware failures. In terms of backup management, Tencent Cloud has formulated backup management procedures to back up important data collected and processed in accordance with relevant legal and regulatory requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			For customer data in the cloud, Tencent Cloud provides multiple storage replicas and backup services for customers based on the functions of cloud products or services, and assumes responsibilities for the provided data backup services in accordance with the agreements in the product service level agreements. Tencent Cloud offers multiple storage services and database services provided by Tencent Cloud all have backup functions, supporting requirements such as multi-redundancy backup and cross-regional disaster recovery, such as: • <u>Cloud Object Storage (COS):</u> Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS):</u> Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS):</u> Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C:</u> Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL:</u> Provides automatic and manual backup options, including cross-region

No.	Domain	Summary of Controls	Tencent Cloud's Response
			backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB</u>: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios.
			Tencent Cloud usually conducts regular emergency response and disaster recovery drills to test service continuity (availability). Based on its business continuity plan, Tencent Cloud formulates drill schemes, carries out drill risk assessments, and formulates corresponding safeguard measures to avoid negative impacts on services due to drills. Tencent Cloud's disaster recovery drills are often conducted by simulating real classic disaster recovery scenarios, including attack and defense competitions and large-scale failures, to comprehensively examine the system's disaster recovery capabilities, response speed, and recovery capabilities. After the drills, relevant departments organize the preparation of drill reports, rectify issues based on improvement measures, and archive and retain the reports. In addition, Tencent Cloud reviews and updates its business continuity management system every year, and reviews the business continuity plans and disaster recovery plans of relevant products and services based on the results of business impact analysis, updating them as needed.
	5.2.2 [Alternative]	Does the provider conduct regular checks to ensure service continuity (availability)?	

6.4.6 Security Incident Response and Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.1	Procedures and System for	6.1.1 [Alternative] Does the provider establish and implement	Tencent Cloud has formulated information security incident management

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Security Incident Response	procedures for responding to security incidents, including hacking and other cyber threats?	specifications for incident response and handling, established information security reporting, response and handling mechanisms and relevant procedures, and clarified the roles and specific responsibilities of each team in the incident handling process. Tencent Cloud records security incidents using an internal security operations system. For detected and identified security incidents, Tencent Cloud analyzes and classifies the incidents based on factors such as the nature of the incident, data sensitivity and scope of impact, and promptly notifies the responsible personnel to follow up and handle the incidents. Tencent Cloud has also established a network security emergency response plan, covering various network security emergency scenarios such as network attacks, malicious programs, data security, equipment and facility failures, and catastrophic events. Based on improving and perfecting the emergency response plan system, supporting the construction of an emergency response team, and focusing on standardizing the emergency response process, Tencent Cloud further enhances its capabilities in monitoring and early warning, notification and disposal, so as to prevent and reduce the adverse impacts of network security incidents on Tencent Cloud.
		6.1.2 [Alternative] Does the provider regularly conduct training based on incident response procedures to ensure prompt response to security incidents?	To ensure the effectiveness and timeliness of the incident response process, Tencent Cloud's internal business departments regularly conduct drills related to security incident emergency plans. Meanwhile, in accordance with the development of security technology and the changing situation, Tencent Cloud provides technical training to employees of the security team to ensure that they understand and comply

No.	Domain	Summary of Controls	Tencent Cloud's Response
			with the latest security regulations and operation procedures, and master the latest information security standards and best practices.
			Tencent Cloud's security team has established a 7×24-hour security operation system, focusing on core scenarios such as vulnerability monitoring, intrusion traceability, and attack blocking. It responds to security alerts in real time and quickly completes attack traceability and the formulation of emergency response plans, effectively curbing the spread of security incidents. Tencent Cloud also provides customers with a series of relevant products or services to assist them in security operations, including: • Cloud Security Center (CSC): As a one-stop security management platform, it helps customers realize a closed-loop security operation covering pre-event threat detection, in-event response and disposal, and post-event traceability analysis through asset center, risk center, alert center, and advanced security management. CSC supports unified security management of cloud assets, including automated asset inventory, security risk detection and identification, and automated response and disposal of security risks. It collects threat alerts and logs from cloud firewalls and Web application firewalls, and uses Tencent Cloud threat intelligence and its own security knowledge base to conduct automated analysis and investigation on the data, providing customers with centralized threat detection, investigation, and disposal capabilities. • Threat Intelligence Center (TIX): As a one-stop intelligence service platform, TIX
	6.1.3 [Required]	Does the provider maintain a support system to enable integrated financial security control?	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			provides three major intelligence capabilities: basic intelligence, attack surface intelligence, and business intelligence. It supports functions such as intelligence query, IOC analysis and judgment, and attack surface management, which can help customers more efficiently analyze and judge security incidents and more comprehensively assess the risk exposure of enterprise assets, helping enterprises build an efficient three-dimensional security defense system. In addition, a variety of log products and services such as Tencent Cloud Log Service (CLS), CloudAudit and Flow Logs enable customers to download cloud logs to local for viewing 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".
6.2	Security Incident Response	6.2.1 [Required] Does the provider promptly inform users of the cause, details, and measures taken regarding security incidents, in accordance with incident response procedures?	Tencent Cloud has established relevant procedures for information security incident response, incident escalation, and incident notification to timely warn or notify relevant parties such as internal company personnel and customers who may or have been affected by the incident, ensuring that all parties can conduct communication and coordination in an orderly, timely and efficient manner. For security incidents that may affect customers, Tencent Cloud will notify customers of the handling and analysis results of the information security incident through appropriate methods after internal review based on the scope and degree of impact of the information security incident. and provide corresponding technical support to assist customers in taking remedial measures to minimize losses.

6.4.7 User Authentication and Access Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.1	Access Control Policy	7.1.1 [Alternative] Does the provider establish and implement an access control policy covering areas, scope, rules, methods, and other access control measures to prevent unauthorized access?	Tencent Cloud has formulated standards for access control management, regulating access control activities for cloud platform products, terminal systems, host operating systems, application systems, and network equipment. Tencent Cloud requires user accounts to use unique identifiers and sets password policies for employee accounts in accordance with security baselines, including password length, complexity, locking, and reset requirements. For internal terminals, operating systems, applications, and network equipment, Tencent Cloud configures login failure limit and session timeout policies.
			Tencent Cloud uses a zero-trust security management system for employee access authentication, and users must complete two-factor authentication before accessing internal resources. It implements real-time security monitoring of employee account login status; once any abnormal login behavior is detected, the IT security system immediately contacts the account holder for verification and handling, and records relevant events in detail.
			Tencent Cloud has also established authorization policies and a segregation of duties matrix mechanism, adhering to the principle of least privilege. 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 personnel identities corresponding to job roles and permission levels for various business systems, and conducts regular internal permission audits to ensure that permissions are not abused or misused.
7.2	Access Right	7.2.1 [Alternative] Does the	Tencent Cloud has formulated access

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Management	provider regularly review the appropriateness of granting access rights, usage (e.g., long-term nonuse), and changes (e.g., retirement, leave of absence, change of duties within the department, job transfer) to effectively manage access to cloud computing systems and critical information? 7.2.2 [Required] Does the provider establish and implement a control mechanism for administrators of information processing systems who possess access to terminals and data related to user data processing system?	control management specifications that clarify authorization policies and a separation of duties matrix mechanism, and maintains records of personnel identities corresponding to job roles and permission levels for various business systems. It strictly adheres to the principle of least privilege and implements least privilege control by default. Regular internal permission audits are conducted to ensure that permissions are not abused or misused. For access permissions that are no longer required, appropriate follow-up actions are taken to revoke unnecessary access permissions in a timely manner. A bastion host has been fully deployed in Tencent Cloud's production environment to centrally manage the administrator account permissions of backend system components. Internal operation and maintenance personnel must obtain authorized approval to access the bastion host, which can only be accessed by specific internal operation and maintenance personnel of Tencent Cloud, and two-factor authentication is required for login. Operation and maintenance logs are centrally stored by the log platform, which are regularly reviewed by Tencent Cloud's internal audit team. Rules for detecting abnormal user operations and activities are defined in the log management platform, and identified abnormalities are automatically pushed to the security team for investigation. In addition, customer data is classified as high-security data within Tencent Cloud. The control of customer data is entirely held by the customer. Unless necessary for service provision or troubleshooting, with explicit customer authorization or in accordance with national laws and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			regulations such as investigations into criminal cases by national or local government departments, Tencent Cloud employees will never proactively access any customer data. Tencent Cloud implements end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services, and establishes real-time monitoring and interception mechanisms to detect and prevent any abnormal data access behaviors.
7.3	User Identification and Authentication	7.3.1 [Alternative] Does the provider offer additional authentication options when requested by cloud computing users? 7.3.2 [Alternative] Does the provider establish and communicate procedures for managing accounts, passwords, etc., to ensure the secure use of cloud computing services?	In terms of cloud user access control management, Tencent Cloud has formulated relevant procedures for access control management, including standards related to the registration, management, and support of cloud customer accounts. It provides access control management functions for cloud customers, allowing customers to independently establish access control policies to manage access to the cloud products they purchase through these policies. Tencent Cloud provides customers with a management console that supports centralized management and control of cloud resources. When customers register a cloud account, each cloud customer is assigned a unique identifiable account and configured with password setting rules/policies, and the management console automatically checks the uniqueness of the user account name. When customers log in to the management console, identity, authentication information, and operation commands are transmitted via the HTTPS protocol. Customers can centrally manage cloud services and data through open APIs. When registering for the Open API function, customers need to use access keys

No.	Domain	Summary of Controls	Tencent Cloud's Response
			assigned to each customer for identity verification. Tencent Cloud supports customers in using multi-factor authentication to enhance the security of account login and any sensitive operations (such as changing account passwords). It also provides functions for resetting and modifying account passwords. Tencent Cloud also provides customers with the Cloud Access Management (CAM) service to help them securely and precisely manage access to Tencent Cloud products and resources. The primary account of a user has full access permissions to resources under its name by default, and can create sub-users and assign identity IDs, credentials, and permissions to them. Users can modify the password rules and single login session timeout of sub-users through the CAM console. To prevent password leakage, Tencent Cloud encrypts customer passwords using SHA256 hashing and salting to avoid storing plaintext passwords. CAM also supports multiple methods of secondary authentication and supports the supervision, compliance inspection, operation audit, and risk review of Tencent Cloud account activities through CloudAudit. Tencent Cloud provides documented operational procedures and user manuals via its official website. Additionally, Tencent Cloud offers Tencent Cloud Training and Certification based on product knowledge and relevant professional expertise to enhance customers' technical capabilities and cloud proficiency. In addition, Tencent Cloud provides customers with multiple channels, including 7x24 hour work orders, 7x24

No.	Domain	Summary of Controls	Tencent Cloud's Response
			hour hotlines, intelligent customer service, and self-service services, to continuously address customer inquiries and feedback. Its customer service team and technical experts provide customers with rapid and effective support.

6.4.8 Virtualization and Infrastructure Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
8.1	Virtualization Security	8.1.1 [Alternative] Does the provider establish a plan for the creation, change, recovery, etc., of virtual resources (e.g., virtual machines, virtual storage, virtual software)?	Tencent Cloud provides customers with a management console that enables centralized management and control of cloud resources. Through the console, customers can perform operations such as purchasing, viewing, and utilizing Tencent Cloud products and services. They can also access recent visits, actively used cloud products, monitoring alerts, pending work orders, outstanding bills, and other related information.
		8.1.2 [Required] Does the provider ensure that when a user deletes virtual resources while using the cloud service,* the removal happens in a way that prevents all deleted resources from being recovered?	When a customer no longer needs an instance, they can terminate the instance. Manually terminated instances are placed in the recycle bin and retained for a maximum of 2 hours. For instances in the recycle bin, customers can renew, restore, or release them according to different scenarios and needs.
		* Includes virtual machines (image, backup, snapshot, etc.), virtual storage, virtual software, and virtual environment configuration information.	Before resource reallocation, Tencent Cloud follows standard policies and contractual requirements to perform thorough logical or physical erasure in a timely manner, ensuring that storage spaces containing sensitive information such as customer identification information, files, directories, and database records are completely cleared before being released or reallocated to other users.
		8.1.3 [Required] Does the provider ensure the soundness of virtual assets and notify users of any	Tencent Cloud's Cloud Virtual Machine (CVM) is a scalable virtualized computing service that allows customers to customize

No.	Domain	Summary of Controls	Tencent Cloud's Response
		damages to virtual resources?	resources such as CPU, memory, hard disk, network, and security. Tencent Cloud provides customers with secure official public images, which include the official genuine basic operating systems and initialization components provided by Tencent Cloud. CVM also supports customers in creating or importing custom images through the image import function, as well as sharing and deleting custom images. Tencent Cloud also provides Cloud Monitor for CVM, which supports various real-time alerts, and offers security services such as DDoS protection, DNS hijacking detection, intrusion detection, vulnerability scanning, web page trojan detection, and login protection. For container image management, the <u>Tencent Cloud Container Registry (TCR)</u> provides customers with secure, dedicated, and high-performance container image hosting and distribution services. Customers can also use the <u>Tencent Cloud Container Security Service (TCSS)</u> to protect the security of containers and images. TCSS supports functions such as container asset management, image security scanning, runtime intrusion detection, and security baseline configuration management, helping customers build a container security protection system and provide full-life-cycle protection for containers from image generation and storage to operation. At the same time, Tencent Cloud provides 7x24-hour operation and maintenance services by a professional team. With advanced server monitoring and diagnosis technologies, it can automatically detect various server faults and automatically trigger repair processes at the first time. Through integrating advanced remote

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management tools, it automatically dispatches on-site data center and vendor resources to restore server faults in a timely manner. For security incidents that may affect customers, Tencent Cloud will notify customers of the handling and analysis results of the information security incident through appropriate methods after internal review based on the scope and degree of impact of the information security incident. and provide corresponding technical support to assist customers in taking remedial measures to minimize losses.
			In terms of physical access control, Tencent Cloud requires data center operators to establish a complete personnel access control security matrix in the access control system to effectively manage various personnel access and operation behaviors. Tencent Cloud also requires security personnel of data centers to inspect each computer room and equipment in strict accordance with inspection lists and plans and equip data centers with 7x24-hour non-blind spot video monitoring and alarm systems manned by security rooms. In terms of logical access control, the production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to 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.
	8.1.4 [Alternative] Does the provider implement security management and access control for physical and logical virtualization servers (e.g., hypervisors) and interfaces?		
	8.1.5 [Required] Does the provider	To strengthen the security management and	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		establish and implement administrative, physical, and technical protection measures for open servers that distribute virtual resource management systems* and virtual software (e.g., apps and application programs)? *Websites that provide virtual resources, such as cloud portals, cloud consoles, and APIs.	control of Tencent Cloud virtual machines and virtual services during use, Tencent Cloud has internally formulated virtualization security management specifications, clarifying relevant standards for virtual machine resource management, permission management, and configuration management. Tencent Cloud builds a virtualization security defense system through multiple technical means such as virtual machine isolation and resource control, patch management and vulnerability protection, and Hypervisor security hardening.
			In terms of security configuration, Tencent Cloud has established internal cybersecurity configuration standards and security baseline standards to standardize security configurations for network devices, firewalls, host operating systems, databases, and application systems. Security policies and parameter settings for network devices such as routers, firewalls, and servers are regularly reviewed to ensure effectiveness.
8.2	Virtual Environment Protection	8.2.1 [Alternative] Does the provider establish and implement malware protection measures to protect users' virtual environments?	In terms of security monitor, Tencent Cloud deploys Endpoint Detection and Response (EDR) tools to comprehensively monitor and control terminal assets of servers across the network. The EDR tools adopted by Tencent Cloud support functions such as antivirus and intrusion detection, security baseline and vulnerability scanning, and security compliance auditing for command operations and login behaviors, and trigger alerts when malicious programs or abnormal behaviors are identified. In terms of vulnerability and penetration testing, Automated scanning tasks are scheduled to identify vulnerabilities in cloud assets, followed by analysis,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			classification, and remediation. The security team conducts large-scale end-to-end penetration tests periodically and targeted tests before major releases or significant changes. To ensure the security of container cloud environments, Tencent Cloud has established a comprehensive, layered container security framework. For north-south network security (between container cloud and external networks), Tencent Cloud leverages traditional security products and capabilities such as Web Application Firewall (WAF), Distributed Denial-of-Service (DDoS) protection, web vulnerability scanning, and Intrusion Detection and Prevention Systems (IDPS) to provide security monitoring and protection. For east-west security (within the container cloud), Tencent Cloud implements container-specific security mechanisms based on principles such as security native integration, security shift-left, and zero trust. A layered security architecture is applied across the infrastructure layer hosting the container cloud platform, the container and container cloud platform architecture layer, and the application layer running on containers.
8.3	Infrastructure Security	8.3.1 [Alternative] Does the provider install and operate information protection systems to secure internal and external networks related to cloud computing services? 8.3.2 [Alternative] Does the provider separate and operate networks while taking tasks, services, and other factors into account? 8.3.3 [Required] Does the provider	To implement network security protection and management, Tencent Cloud has established network security management specifications and a network in-depth defense system. Tencent Cloud clarifies network security control and protection standards, as well as corresponding roles and responsibilities, through management systems and processes, ensuring the safe operation of services carried on Tencent Cloud's network. At the same time, Tencent Cloud designs a network security architecture with reference to industry

No.	Domain	Summary of Controls	Tencent Cloud's Response
		offer features necessary to protect users' virtual environments and enable network segmentation?	practices, divides security domains according to business functions and security risks, physically or logically isolates different security domains, and ensures the security of office networks, production networks, etc. through measures such as access control and boundary protection. Tencent Cloud adopts multiple protection mechanisms such as firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS protection, and web security protection to timely detect, filter, and block malicious network traffic, protecting Tencent Cloud's network security. In terms of network communication 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 terms of isolation, Tencent Cloud adheres to the principle of "data privacy" and uses multi-level technical isolation measures, such as virtualization control layer resource access control strategies, isolation strategies between private networks within the cloud platform, web console permission allocation and authentication, and security mechanisms such as interface session IDs and access keys, to technically ensure that tenants cannot access, obtain, or tamper with data from other tenants. Customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. In addition, Tencent Cloud also provides customers with a variety of services for effective network security management, such as: • <u>Tencent Cloud EdgeOne</u>, 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. • <u>Cloud Firewall (CFW)</u> 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. • <u>Web Application Firewall (WAF)</u> helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. • <u>Anti-DDoS</u> combines abundant, high-quality DDoS mitigation resources with continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			ensuring stable and secure business operations.

6.4.9 Development and Operation Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.1	System Analysis and Design	9.1.1 [Alternative] Does the provider synchronize with a standard time to ensure the accuracy of security audit logs?	Tencent Cloud provides the current accurate Coordinated Universal Time (UTC) through the Network Time Protocol (NTP). Tencent Cloud offers intranet NTP servers for use by instances on Tencent Cloud, and customers can use the public network NTP servers provided by Tencent Cloud for non-Tencent Cloud devices. Furthermore, Tencent Cloud regularly checks the time synchronization status of NTP servers to ensure unified, accurate, and reliable time across the entire network.
9.2	Implementation and Testing	9.2.1 [Alternative] Does the provider prohibit the use of user data during testing (In the event of unavoidable circumstances such as load testing, the user information is converted and used for the test, and the information is immediately deleted)?	Tencent Cloud designs its network security architecture by referring to industry practices, divides security domains based on business functions and security risks, isolates different security domains physically or logically, and ensures the security of office networks, production networks, etc. through measures such as access control and boundary protection. Tencent Cloud prohibits the use of unsensitized production data in the development/testing environment. In addition, customer data is classified as high-security data within Tencent Cloud. Customers hold exclusive ownership and control over their own data content. Unless it is necessary to provide services or troubleshoot, and with the explicit authorization of customers or in accordance with national laws and regulations such as investigations into criminal cases by national or local government departments, employees of Tencent Cloud will never proactively access any customer data.

6.4.10 Encryption and Data Protection

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.1	Data Protection		Tencent Cloud has established data security management procedures, clarifying the principles of data classification, grading, and data protection. It requires data owners to implement corresponding security protection measures throughout the entire lifecycle of data collection, transmission, access control, backup, transaction protection, and information transmission management with third parties in accordance with the requirements of data classification and grading, so as to protect the confidentiality, integrity, and availability of data. The classification of Tencent Cloud electronic data includes customer cloud business data, Tencent Cloud data, and privacy data. Among them, customer cloud business data refers to the business data information of customers (cloud tenants) on the cloud; Tencent Cloud data refers to the data generated by operating and maintaining Tencent Cloud services; and privacy data refers to the personal data provided by customers when using cloud services. In addition, customer data is classified as high-security data within Tencent Cloud, and customers have the sole ownership and control over their own data content. Unless it is necessary to provide services or troubleshoot, and with the explicit authorization of customers or in accordance with national laws and regulations such as investigations into criminal cases by national or local government departments, Tencent Cloud employees will never proactively access any customer data.
		10.1.1 [Alternative] Does the provider classify and manage data according to data classification criteria?	
		10.1.2 [Alternative] Does the provider clearly define user data ownership?	Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			control over their data content. 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 agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions.
			As a cloud service provider, Tencent Cloud ensures the integrity of user data throughout its entire lifecycle—including input, output, transmission, exchange, and storage—through technical measures, management systems, and security architecture design. Regarding data storage integrity assurance, when storing data, Tencent Cloud adopts multi-copy redundant storage and erasure code technology, and takes necessary recovery measures immediately when integrity errors are detected, thereby improving the fault tolerance of data. At the same time, Tencent Cloud provides professional 7x24-hour operation and maintenance services. With advanced server monitoring and diagnosis technologies, it can automatically detect various server faults and trigger the repair process at the first time. By integrating advanced remote management tools, it automatically dispatches on-site data center and vendor resources to restore server faults in a timely manner.
	10.1.3 [Alternative]	Does the provider ensure the integrity of data during input, output, transmission, exchange, and storage at all times?	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Regarding data transmission integrity assurance, all communications on the Tencent Cloud console are encrypted and protected by the HTTPS security protocol. The cloud API interfaces provided by Tencent Cloud's products also feature security capabilities such as HTTPS encryption, signature verification, and status monitoring, preventing data from being tampered with, lost, or injected with unauthorized content during transmission and exchange, thereby ensuring the integrity and trustworthiness of the data transmission.
			The Tencent Cloud Console provides customers with secure permission allocation and sub-user management through Cloud Access Management (CAM), helping customers conveniently control the specific operations that users and roles can perform and the resources they can access. Customers can enable two-factor authentication for the primary account and its subordinate sub-accounts through CAM to enhance account security, and use CloudAudit to record logs, continuously monitor and retain user activities and API usage related to operations in the entire Tencent Cloud infrastructure. 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 owned by users are the minimum necessary to access assets and complete work tasks. The Bastion Host also supports operation audit functions, recording and analyzing users' operation logs to ensure effective traceability of security incidents.
	10.1.4 [Alternative]	Does the provider offer users data access control and data processing protection features, such as forgery prevention?	Customers can also use the Data Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			<u>Audit (DSA)</u>. DSA is an artificial intelligence-based database security audit system. It supports full auditing and warehousing of various session information, access operations, and SQL statements of databases in enterprise networks, identifies malicious behaviors in operations based on multiple rule bases and threat detection engines, and promptly notifies administrators to take corresponding security protection measures. In terms of anti-forgery, Tencent Cloud provides customers with <u>SSL Certificates</u> service. Cooperating with top-level Certificate Authority (CA) institutions and agents, it provides HTTPS solutions for customers' websites and mobile applications. SSL Certificates offers a one-stop service for SSL certificates, including certificate application, management, and deployment. It also supports customers to upload SSL certificates issued by any institution for unified management of all certificates and monitoring the validity period of each certificate. In addition, multiple Tencent Cloud storage and database products support data encryption functions, adopt secure high-strength encryption algorithms, and implement full lifecycle management of keys by integrating with the <u>Key Management Service (KMS)</u>. KMS uses FIPS-140-2 certified Hardware Security Modules (HSM) to generate and protect keys, and supports the full lifecycle management of customers' encryption keys. Tencent Cloud has also formulated internal access control management specifications and established a permission management and authorization mechanism. It strictly adheres to the principle of least privilege

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and implements least privilege control by default. Tencent Cloud implements real-name verification and maintenance throughout all nodes for data access permissions to ensure the integrity of data assets and the reliability of business services, and establishes real-time monitoring and interception mechanisms to detect and prevent any abnormal data access behaviors. It also conducts regular internal permission audits to ensure that permissions are not abused or misused. A bastion host has been fully deployed in Tencent Cloud's production environment to centrally manage the administrator account permissions of backend system components of Tencent Cloud. Access to the bastion host requires authorized approval and can only be accessed by specific internal operation and maintenance personnel of Tencent Cloud. Operation and maintenance logs are centrally stored by the log platform and reviewed regularly by Tencent Cloud's internal audit team. For multi-tenant data isolation, Tencent Cloud adheres to the principle of "data confidentiality" and ensures that tenants cannot access, obtain, or tamper with other tenants' data through security mechanisms such as virtualization control layer resource access control strategies, isolation strategies between private networks within the cloud platform, permission allocation and identity verification on the Web console, and interface session ID and access keys.
		10.1.5 [Alternative] Does the provider offer measures to track the location where user data is processed?	Tencent Cloud's infrastructure is deployed in multiple locations globally, consisting of regions and availability zones. Each region is an independent geographic area, and each availability zone is an independent fault maintenance domain with physical

No.	Domain	Summary of Controls	Tencent Cloud's Response
			isolation between availability zones. Customers can flexibly deploy data and systems in different regions or availability zones according to their business development needs and data security requirements. Adhering to the principle of openness and transparency, Tencent Cloud will promptly provide customers with information through appropriate channels if customers need to know about the location of data storage, including the location of data centers where data is stored, the cold backup status of data, and the storage location of cold backup data.
		10.1.6 [Required] Does the provider irreversibly delete all virtual resources associated with the user upon termination of the cloud service use agreement?	If customers need to terminate the service agreement due to business changes or future IT planning, they can choose to back up and migrate cloud data and production environments at any time. After the customer's service is terminated, Tencent Cloud will completely delete customer data including copies and backups after the retention period expires in accordance with the strict data erasure methods, and the deleted data cannot be recovered.
10.2	Encryption	10.2.1 [Alternative] Does the provider protect user data by applying encryption technology when processing it? 10.2.2 [Alternative] Does the provider establish secure encryption key management procedures and store keys safely?	Multiple Tencent Cloud storage and database products support data encryption functions, adopt secure high-strength encryption algorithms, and implement full lifecycle management of keys by integrating with the Key Management Service (KMS) to ensure data confidentiality. KMS uses FIPS-140-2 certified Hardware Security Modules (HSM) to generate and protect keys, and supports the full lifecycle management of customers' encryption keys. To reduce the risk of key cracking or abuse, KMS supports key rotation and adopts secure and reliable methods to delete invalid, revoked, or leaked keys. Deleted keys cannot be

No.	Domain	Summary of Controls	Tencent Cloud's Response
			recovered, and the encrypted data under such keys cannot be decrypted. Multiple Tencent Cloud storage and database products support data encryption functions, adopt secure high-strength encryption algorithms, and implement full lifecycle management of keys by integrating with the Key Management Service (KMS) to ensure data confidentiality. KMS uses FIPS-140-2 certified Hardware Security Modules (HSM) to generate and protect keys, and supports the full lifecycle management of customers' encryption keys. To reduce the risk of key cracking or abuse, KMS supports key rotation and adopts secure and reliable methods to delete invalid, revoked, or leaked keys. Deleted keys cannot be recovered, and the encrypted data under such keys cannot be decrypted.

6.4.11 Physical Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
11.1	Physical Protection Area	11.1.1 [Required] Do major facilities in the computer room house equipment for access control and monitoring control?	In terms of access management for secure areas, Tencent Cloud requires data center operators to establish a complete personnel access control security matrix in the access authorization system based on personnel categories and access permissions, so as to effectively manage the access and operation behaviors of various personnel. Operators are required to verify the identities of all visitors and staff entering and exiting the data center, conduct inspections of their personal belongings, and register the items they carry. For security and monitoring, Tencent Cloud requires operators to arrange security personnel to inspect each computer room and equipment in strict accordance with inspection lists and plans, sign and record

No.	Domain	Summary of Controls	Tencent Cloud's Response
			the inspection time at each check point, and immediately activate the data center emergency response process once infrastructure failures or security incidents are identified. Operators are also required to equip data centers with a 7x24-hour non-blind spot video monitoring and alarm system manned by a security room, with monitoring records securely stored for an adequate period.
		11.1.2 [Required] Does the provider restrict (control) the use of wireless communication networks within the computer room when processing unique identification or personal credit information?	Tencent Cloud has implemented security policies for its wireless network, requiring employees to undergo identity verification when logging onto the wireless network. Meanwhile, the enterprise IT management backend conducts regular checks on wireless SSIDs and access points (APs); if illegal SSIDs or APs are detected, an alert is sent to relevant IT administrators for handling. And the installation of wireless telecommunication networks is prohibited in the production environment.
		11.1.3 [Alternative] Does the provider establish and implement physical protection measures for offices and facility spaces?	In terms of physical environment security, Tencent Cloud has formulated physical security management systems to standardize operational safety, identify risks in a timely manner, and strengthen physical security management. Tencent Cloud classifies the company's secure areas into critical secure areas and general secure areas, and sets up security perimeters, access control and inspection measures, as well as video surveillance equipment. Employees are required to maintain the security of information assets in the office environment, including properly storing paper documents containing sensitive information. Terminal devices used by Tencent Cloud employees are equipped with lock screen policies to lock the devices

No.	Domain	Summary of Controls	Tencent Cloud's Response
			when employees leave them. Unattended equipment such as copiers, fax machines, shredders, and printers is placed in monitored and appropriate areas of the office to prevent unauthorized use and intrusion.
			Currently, Tencent Cloud operates two data centers in South Korea, providing a variety of cloud computing services including Cloud Virtual Machines (CVM), Cloud Databases, and CDN. South Korean customers can choose to store and process their data locally in South Korea.
11.2	Protection of Information Processing Facilities and Devices	11.2.1 [Required] Does the provider ensure that all information processing systems processing unique identification and personal credit information are located in Korea?	Tencent Cloud strictly abides by the laws and regulations of the jurisdictions where it operates its business and has established security and compliance-related procedures to ensure that information security operations meet the requirements of relevant laws, regulations, standards, and procedures. In addition, adhering to the principle of openness and transparency, Tencent Cloud will promptly provide customers with relevant information through appropriate channels if they need to know the location of data storage and other related information. For more information on the collection, processing, and sharing of personal information by Tencent Cloud, please refer to the Privacy Policy.
		11.2.2 [Required] Is the provider equipped with necessary equipment, such as fire detectors, firefighting devices, water leakage detectors, thermo-hygrostats, uninterruptible power supplies (UPS), and dual power lines, to prepare for natural or man-made disasters (e.g., fire, water leakage, power anomalies) depending on	As a cloud service provider, Tencent Cloud is committed to providing customers with secure, stable, continuous, and reliable physical infrastructure. All data centers globally operated by Tencent Cloud are selected, constructed, or leased in accordance with relevant international standards and local security requirements. Tencent Cloud has deployed two leased data centers in South Korea.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the importance and characteristics of each security area?	Tencent Cloud requires operators to equip data centers with complete fire protection systems, including fixed-area fire detection systems, automatic fire extinguishing systems, and manual fire extinguishing devices for emergency use. Operators are also required to configure data centers with lightning protection systems, radiation protection systems, power supply and distribution systems, UPS systems, lighting systems, and other facilities necessary for the normal operation of computer rooms. Maintenance personnel at data centers work in shifts to ensure all-weather maintenance and rapid resolution of equipment failures.
		11.2.3 [Alternative] When discarding equipment from information processing facilities that store user information, does the provider proceed in the manner that recovery is not feasible?	When media used to provide Tencent Cloud services need to be replaced due to failure or scrapped upon reaching the end of their service life, Tencent Cloud follows strict procedures in a timely manner and adopts secure physical destruction methods to ensure that hard drives are completely destroyed, with records of the destruction duly registered.

6.5 Task Continuity Plan for the Use of Cloud Computing Services

Appendix 2-3 Task Continuity Plan for the Use of Cloud Computing Services contains measures to be planned and implemented for business continuity by financial companies or electronic financial service providers in the course of using cloud services, which are divided into “Essential Measures” and “Additional Measures”. Pursuant to subparagraph 1 of paragraph (1) of Article 14-2 of these Regulations, if the cloud computing service used is classified as a material business, financial companies or electronic financial service providers shall comply with both “Essential Measures” and “Additional Measures”; if the cloud computing service used is classified as a non-material business, they may comply with “Essential Measures” only.

As the “Essential Measures” in Appendix 2-3 are quotations from the original provisions of these Regulations, the corresponding compliance responses can be found in the relevant sections of this Guide: [Section 6.1 Securing the Safety of Electronic Financial Transactions and Protecting Users](#); [Section 6.2 Licensing, Registration, and Operations of Electronic Financial Affairs](#), and [Section 6.3 Supervision of Electronic Financial Affairs](#).

This chapter will focus on the “Additional Measures” in Appendix 2-3 and describe how Tencent Cloud, as a cloud service provider, assists financial companies and other relevant entities in complying with the relevant requirements.

No.	Domain	Summary of Controls	Tencent Cloud’s Response
1	System Failure Preparation (e.g., Data Backup)	[Essential Measures]: Article 13(1)4: Establishing and implementing a plan to safely carry out and urgently destroy auxiliary memory devices and other computer data in an emergency; Article 13(1)6 through 7: 6. Regularly backing up computer data according to their priority levels for putting the backup files in a remote safe deduplication storage, and keeping and managing a record of the backup files;. 7. Regularly verifying major backup files of computer data. Article 14(1) through (3): 1. Create and store each of the following items A. Operating Manual for Major Information Processing Systems B. Director of Maintenance Management who recorded the implementation of regular maintenance for major information processing systems C. Department of Persons Responsible for Information Processing Systems and Disability Situation Registry. 2. Building a monitoring system to monitor, issue warning against, and control the state of the system resources, which will help ascertain whether the information processing system functions normally;	When conducting backups, customers shall include important configuration files related to cloud services, virtual system images, and other items into the scope of data backup objects. Various cloud products and services provided by Tencent Cloud, such as computing services, network services, container and middleware services, feature high availability, ensuring that customers can quickly respond to and restore key functions in the event of a cyber security incident, such as: • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM’s cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data. Meanwhile, multiple storage services and database services provided by Tencent Cloud are equipped with backup functions to meet various backup needs of customers, such as: • <u>Cloud Object Storage (COS)</u>: Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		3. Establishing and complying with control procedures to prevent information processing system failures due to any errors, etc. at the time of integrating, converting or redeveloping the system. Article 14(5): Regularly backing up the operating systems, details of configuration, etc. of the information processing system according to their priority levels and putting the backup files in a remote safe deduplication storage, and keeping and managing a record of the backup files for at least one year; Article 50(1)3: Having the backup devices to prevent the loss of computer data from any computer system failure; [Additional Measures]: Data backup includes key configuration files related to cloud service, virtual system images, etc.	accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS)</u>: Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS)</u>: Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C</u>: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL</u>: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB</u>: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios. To assist customers in complying with regulatory requirements, Tencent Cloud has internally formulated a backup management procedure to back up important data collected and processed in accordance with relevant legal and regulatory requirements. For internal important information, Tencent Cloud formulates different data backup strategies based on data levels and regularly conducts recovery tests. Tencent Cloud backs up configuration files, logs, and other

No.	Domain	Summary of Controls	Tencent Cloud's Response
			information of servers, network equipment, and application systems in accordance with backup strategies to ensure timely recovery in case of file damage.
2	Redundancy or Standby Equipment	[Essential Measures]: Articles 23(3) and (7): (3) Each financial company and electronic financial business operator shall examine the effectiveness, appropriateness, etc. of the plan to ensure business continuity under paragraph (1) at least once a year and update and manage it. (7) Each financial company and electronic financial business operator shall duplicate the central processing unit, data storage unit, and other main computer equipment or secure reserve devices therefor. [Additional Measures]: Redundant design and configuration plans that consider geographical characteristics and the possibility of concurrent failures related to the provision of cloud computing services.	Customers should design and implement redundancy mechanisms considering factors such as the geographic characteristics of cloud services and the possibility of simultaneous failures. Tencent Cloud data centers cover Mainland China, Asia Pacific, North America, and Europe, and are composed of regions and zones. Different regions of Tencent Cloud are completely isolated from each other, and each region is further divided into multiple isolated zones. Currently, Tencent Cloud has two geographically independent data centers with separate power and network infrastructure in South Korea, which can support customers in storing, processing, and backing up data within South Korea. Customers can flexibly deploy and back up data and systems across different regions or zones according to their business development needs and data security requirements to ensure business disaster recovery requirements. Various cloud products and services provided by Tencent Cloud, including computing services, network services, storage services, database services, container and middleware services, feature high availability, helping customers achieve high availability of systems or services, such as: • <u>Cloud Load Balancer (CLB)</u> provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service

No.	Domain	Summary of Controls	Tencent Cloud's Response
			capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Cloud Object Storage (COS)</u> provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • <u>Cloud Native Database TDSQL-C</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 reliability and availability with robust automatic backup and lossless recovery mechanisms. • <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data. To ensure the continuous availability of customer services, Tencent Cloud requires cloud products to adopt a multi-data center

No.	Domain	Summary of Controls	Tencent Cloud's Response
			redundancy mechanism within a single region to ensure business continuity of cloud services. Tencent Cloud also sets up redundancy or hot standby mechanisms for hardware devices such as servers, network equipment, and security equipment to ensure no data loss and business recoverability in the event of hardware failures.
3	Training and Incident Management	[Essential Measures]: Articles 15(4): Each financial company and electronic financial business operator shall take appropriate measures to promptly cope with damage caused by any hacking or other electronic trespass. Articles 16: Each financial company and electronic financial business operator shall establish and implement measures to prevent malicious code infections, promptly take necessary measures to minimize the spread of and damage from the malicious code. Articles 23(1): Each financial company and electronic financial business operator shall formulate and observe a plan to ensure business continuity in order to prevent his/her or its business from being suspended in emergency situations, such as system failures, disasters, strikes and terror, including the following: 1. Procedures for response to each situation; 2. Plan for recovery from disasters utilizing backups or the disaster recovery center; 3. Composition and management	Customers shall include the roles, responsibilities, and emergency contact information of cloud service providers in the plans for incident management and related drills. To assist customers in meeting regulatory requirements, Tencent Cloud's business continuity procedures clarify internal and external communication strategies during disaster incidents and establish multi-channel communication methods, including console announcements, official websites, in-site messages, SMS, and emails, to promptly release information on events that may affect customers. Tencent Cloud provides ticket services through the cloud console, allowing customers to report faults, incidents, issues, and complaints related to security, availability, and confidentiality. The Tencent Cloud ticket system assigns priorities to customer tickets through a graded response mechanism. When frontline technical teams cannot effectively resolve issues, the system automatically triggers a service escalation process, with product or technical teams intervening for collaborative handling to ensure timely response and resolution of customer needs or feedback. Tencent Cloud also provides online and phone channels on its official website for customers to report problems encountered when using Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		of an emergency response organization; 4. Conditions and procedures for input on his/her or its behalf, handwork, etc.; 5. Conducting simulated training; 6. Building an emergency liaison system with related institutions and enterprises; 7. Scope of and procedures for reporting and external communication. 8. Ensuring and operating emergency support personnel. Articles 23(3) through (6): (3) Each financial company and electronic financial business operator shall examine the effectiveness, appropriateness, etc. of the plan to ensure business continuity under paragraph (1) at least once a year and update and manage it. (4) Any financial company designated by the Financial Services Commission in accordance with the Basic Guidelines for National Emergency Management shall develop and observe an emergency response action manual (hereinafter referred to as "action manual") according to the Finance and Computer Sector Emergency Response Manual of the Financial Services Commission and notify the Financial Services Commission thereof. (5) Each financial company and electronic financial business	services. It has a multi-region backup customer service center that can handle customer inquiries and demands 24/7, delivering high-quality, round-the-clock technical support. Additionally, customers can select applicable service plans to obtain exclusive support including exclusive support groups, dedicated technical service managers, and value-added services. In terms of local support, Tencent Cloud appoints information security liaison officers. Regional information security liaison officers maintain smooth communication with local regulatory authorities and customers in accordance with compliance and business requirements to ensure Tencent Cloud's compliance with legislation, regulations, and contractual agreements. Furthermore, where appropriate, Tencent Cloud can also provide technical support for customers' security drills.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		operator not expressly designated by the Financial Services Commission shall establish and operate an emergency plan to prevent the paralysis of the computer system due to natural disasters, human-induced disasters, technical disasters, electronic trespass, etc. and to ensure prompt recovery from such disasters. (6) Action manuals referred to in paragraph (4) or emergency plans referred to in paragraph (5) shall reflect a plan to ensure business continuity under paragraph (1). Articles 23(8) through (10): (8) Financial companies and electronic financial service providers designated under this paragraph shall establish and operate a disaster recovery center equipped with appropriate scale and personnel, located in a safe place at a sufficient distance from the primary computing center, to ensure business continuity and prepare for the paralysis of the computing center due to system failures or natural disasters. (9) A financial company referred to in any subparagraph of paragraph (8) shall select core business after analyzing the significance of ensuring business continuity according to each business, and determine the restoration time for each business. In such cases, the restoration time for core business shall be less than three hours and that for core business of insurance companies under the Insurance	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Business Act, less than 24 hours. (10) Any financial company that operates a disaster recovery center under paragraph (8) shall conduct disaster recovery training, at least once a year, assuming that the disaster recovery center actually functions. Articles 24(1) through (4): (1) Each financial company or electronic financial business operator shall conduct emergency response training once a year in accordance with the action manual referred to in Article 23 (4) or the emergency plan referred to in Article 23 (5) and report the results to the Financial Services Commission. Each financial company or electronic financial business operator may conduct emergency response training along with the disaster recovery training referred to in Article 23 (10). (2) The Financial Services Commission may select financial companies or electronic financial business operators to conduct joint financial sector emergency response training in order to reinforce the capability of the financial sector to respond to emergency situations. (3) In conducting joint emergency response training under paragraph (2), the Financial Services Commission may request the following institutions to provide assistance: 1. The National Intelligence Service (National Cyber Security Center) under	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Article 17 of the Government Organization Act; 2. The National Police Agency (Cyber Terror Response Center) under Article 12 of the Police Act; 3. The Computer Security Incident Response Team; 4. Other institutions deemed necessary by the Financial Services Commission to secure the effectiveness of emergency response training. (4) A financial company or electronic financial business entity may request cooperation from subsidiary electronic financial business operators to fulfill the obligations specified in Paragraphs (1) and (2). Articles 37-6(5): (5) Each financial company and electronic financial business operator shall formulate and execute a computer security incident response and recovery training plan at least once a year to ensure the ability to respond to computer security incidents; and shall submit the plan and the results thereof to the head of the relevant computer security incident response team: Provided, That this shall not apply to the following financial companies: 1. Credit unions among financial companies referred to in subparagraph 3 (a) of Article 2 of the Act; 2. Financial companies referred to in subparagraph 3 (c) and (d) of Article 2 of the Act; 3. Cooperatives referred to in subparagraphs 4 through 6 of	

No.	Domain	Summary of Controls	Tencent Cloud's Response
4	Establishment of Emergency Measures	Article 2 of the Enforcement Decree;	
		4. Financial companies meeting requirements referred to in Article 5 (2) of the Enforcement Decree.	
		[Additional Measures]: Plans for training and incident management that define the roles, responsibilities, and emergency contact networks of cloud computing service providers.	
		[Essential Measures]: Article 23(5): Each financial company and electronic financial business operator not expressly designated by the Financial Services Commission shall establish and operate an emergency plan to prevent the paralysis of the computer system due to natural disasters, human-induced disasters, technical disasters, electronic trespass, etc. and to ensure prompt recovery from such disasters.	Customers shall formulate supply replacement plans, exit strategies, etc., to respond to major events such as contract changes and bankruptcy, and ensure business recoverability.
		[Additional Measures]: Supply substitution plans for major events such as contract changes and bankruptcy, and exit strategies such as identifying the possibility of task or business recovery.	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 agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions.
			If customers need to terminate the contract due to business changes or future IT planning, they may choose to back up and migrate data in the cloud and the production environment at any time. Tencent Cloud supports customers in backing up or migrating data using a common standard format, so customers can use the same transmission methods and protocols as in

No.	Domain	Summary of Controls	Tencent Cloud's Response
			the cloud migration stage, or use network service products such as Direct Connect (DC) and VPN Connection to ensure the security and reliability of data during the off-cloud migration process. In accordance with the service agreement reached between Tencent Cloud and the customer, if the cloud service expires or is terminated, the customer shall complete the migration of data stored in the cloud servers due to the use of Tencent Cloud services before the expiration of the retention period. After the termination of the cloud service, Tencent Cloud will thoroughly delete customer data including copies and backups after the expiration of the retention period in strict accordance with the specified data erasure method, and the deleted data cannot be recovered. Regarding notifications of changes or termination of products/services, Tencent Cloud will notify customers through announcements, emails, internal messages on the Tencent Cloud console, or other appropriate channels, and release information on functions, versions, changes, etc. of products or services to the public.

6.6 Safety Measures for the Use of Cloud Computing Services

Appendix 2-4 Safety Measures for the Use of Cloud Computing Services contains security measures to be taken by financial companies or electronic financial service providers during the use of cloud services to prevent cloud service-related security incidents, which are divided into “Essential Measures” and “Additional Measures”.

Pursuant to subparagraph 1 of paragraph (1) of Article 14-2 of these Regulations, if the cloud computing service used is classified as a material business, financial companies or electronic financial service providers shall comply with both “Essential Measures” and “Additional Measures”; if the cloud computing service used is classified as a non-material business, they may comply with “Essential Measures” only.

As the “Essential Measures” in Appendix 2-4 are quotations from the original provisions of these Regulations, the corresponding compliance responses can be found in the relevant

sections of this Guide: [Section 6.1 Securing the Safety of Electronic Financial Transactions and Protecting Users](#); [Section 6.2 Licensing, Registration, and Operations of Electronic Financial Affairs](#), and [Section 6.3 Supervision of Electronic Financial Affairs](#). This chapter will focus on the “Additional Measures” in Appendix 2-4 and describe how Tencent Cloud, as a cloud service provider, assists financial companies and other relevant entities in complying with the relevant requirements.

No.	Domain	Summary of Controls	Tencent Cloud’s Response
1	Account Management	[Essential Measures]: Article 13(1)1: Appropriate access management and control procedures shall be established and operated. Article 13(1)11: If a user is subject to a personnel change, such as transfer of post or retirement, immediately controlling the user's access to the information processing system in such a manner as to delete, or suspend the use of, his/her user account or to change a user account shared with him/her. Article 13(2): If sharing a user account is inevitable, the details of access shall be recorded and managed for each individual. Article 14(6): Implementing mandatory procedures for additional authorization in addition to the account and password in cases of logging into the account of the operating system of an information processing system. Establishing a regular monitoring system on the rights of use, records of access, details of work, etc. on the account of the operating system of an information processing system, and taking necessary control measures immediately when strange symptoms appear. Article 17(2): Assigning user	Customers should implement security measures such as two-factor authentication for administrator accounts accessing the cloud management console. In terms of cloud user access control management, customers are provided with access control features that enable them to define and enforce their own access policies for managing the cloud services they have purchased. Tencent Cloud provides customers with a management console, supporting centralized management and control of 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. Tencent Cloud provides a Cloud Access Management (CAM) service to help customers securely and granularly manage access to Tencent Cloud products and resources. The primary account has full access to all associated resources and can

No.	Domain	Summary of Controls	Tencent Cloud's Response
		accounts available for an open-source web server only to business-related persons, and adopting an additional means of authentication, in addition to IDs and passwords. [Additional Measures]: Implementation of enhanced security measures, such as dual factor authentication for administrator accounts accessing a cloud management console.	create sub-accounts, assign identity credentials, and define permissions. Customers can configure password policies and session timeout settings for sub-accounts via the CAM console. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to encrypt passwords, avoiding plaintext storage. CAM also supports various MFA methods and integrates with CloudAudit to track and review user activity logs. Tencent Cloud also provides Bastion Host (BH) to assist customers with user management, authorization management, and comprehensive auditing. Bastion Host can offer different types of authentication methods, such as static passwords and LDAP, based on the actual needs of user scenarios. To enhance security, Tencent Cloud Bastion Host supports two-factor authentication for users. To help customers comply with 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. 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. Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system

No.	Domain	Summary of Controls	Tencent Cloud's Response
			components. Internal 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.
2	Access Control	[Essential Measures]: Article 13(1)2 to 3: 2. Managing the status of computer data held, and designating and managing the responsible person. 3. Controlling the carrying of computer data and computer equipment out of or into the premises. Article 13(3): Each financial company and electronic financial business operator shall establish and implement appropriate measures to manage a data processing system administrator authorized to access terminals and computer data: Provided, That any activity performed by the data processing system administrator in relation to his/her major duties shall be cross-checked and monitored by the responsible person pursuant to Article 28 (2). Article 19-2: Financial companies or electronic financial service providers must establish procedures and methods for the injection, operation, renewal, and destruction of keys (including passwords or keys of authentication systems, etc., used to verify the authenticity and integrity of programs) applicable	Customers should establish written documentation for accessing cloud resources and restrict access to console administrator accounts to be conducted only from isolated, dedicated terminals. Tencent Cloud provides documented operational procedures and user manuals via its official website. Additionally, Tencent Cloud offers Tencent Cloud Training and Certification based on product knowledge and relevant professional expertise to enhance customers' technical capabilities and cloud proficiency. Regarding the access control of privileged accounts, Tencent Cloud offers Bastion Host (BH), which enables granular authorization based on user, asset, account, and operational permissions, ensuring that users only have the minimum privileges necessary to access assets and perform their tasks. Bastion Host can serve as a unified entry point for managing and maintaining internal assets and also supports operation auditing by recording and analyzing user activity logs to ensure effective traceability of security events. To support customers in complying with regulatory requirements, Tencent Cloud has clearly defined the management requirements and corresponding authorization mechanisms for special access privileges internally. Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		to cryptographic and authentication systems, and manage these keys securely. [Additional Measures]: Documentation of procedures for accessing cloud systems and measures to ensure that console administrator accounts can only be accessed only from a separate terminal.	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. All backend operation records are stored centrally on a logging platform and reviewed periodically by Tencent Cloud's internal audit team.
3	Network Security	[Essential Measures]: Article 15(1)3: Separating, blocking, and prohibiting internal business systems connected to internal communication networks from connecting to external communication networks, such as the Internet (including wireless networks): Provided, that this shall not apply to the following cases: (a) Research and development activities that do not process users' unique identification information or personal credit information (However, this is only applicable if a financial company or electronic financial business entity has conducted its own risk assessment and applied the network separation alternative information protection control set by the Governor of the Financial Supervisory Service); (b) Situations deemed inevitable for business purposes and confirmed by the Governor of the Financial Supervisory Service. Article 15(6)1: Minimizing the scope of affairs conducted using a wireless communications network, which shall be designated in	Customers should implement encryption measures for information storage and transmission based on regulatory requirements, and develop and execute a security management plan covering the entire lifecycle of cryptographic keys. Customers should identify and manage data interactions between internal systems and cloud systems, and implement encryption for the main communication channels both between systems and within the cloud services. 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: • <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-

No.	Domain	Summary of Controls	Tencent Cloud's Response
4	Linking the Cloud Service System with the Organization's Internal Systems	advance with approval from the chief information security officer designated under Article 21-2 of the Act; Article 17(1): Ensuring that an open web server is established within an independent communications network (hereinafter referred to as "DMZ") between his/her or its internal and external communications networks to protect it as a means of network and web access control; Article 18: Each financial company and electronic financial business operator shall establish and implement appropriate measures, including those related to the address system, allocation, and management, to ensure the secure use of information provider addresses (hereinafter referred to as "IP addresses"), and shall keeping and preserving a separate record that indicates the details of Internet access using his/her or its internal and external IP addresses, for at least one year. [Additional Measures]: Encryption of primary communication channels in cloud computing services and interconnection between systems	premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • <u>Cloud Connect Network (CCN):</u> 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.
		[Essential Measures]: Article 12(1) to (4): 1. Taking measures to prevent anyone other than responsible staff from accessing the terminals without authorization. 2. Keeping records that make it possible to verify whether	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		terminals accessing the information processing system are used by persons authorized to use them. 3. Designating major terminals to which more intense protective measures are applied, such as prohibiting their removal out of the premises, logging on to the Internet, and the logging on to groupware and regular verification of malicious code infection. 4. Controlling access to auxiliary memory devices or portable computer equipment from terminals so as to prevent divulgence of information, malicious code infections, etc. Article 15(1)5: Physically separating the information processing system located in computer rooms and the terminals directly connected for operation, development, and security purposes from any external communication networks, such as the Internet: Provided, that this shall not apply to the following cases: (a) Research and development activities that do not process users' unique identification information or personal credit information (However, this is only applicable if a financial company or electronic financial business entity has conducted its own risk assessment and applied the network separation alternative information protection control set by the Governor of the Financial Supervisory Service); (b) Situations deemed inevitable for	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		business purposes and recognized by the Governor of the Financial Supervisory Service. Article 34(1): Encrypted communications shall be used for electronic financial transactions, except telephones or other means of communications to which encryption itself cannot be applied in view of the nature of a means of transactions (Provided, That this shall not apply where private lines are used and self-examinations of security levels thereof has been conducted pursuant to Article 36) Article 60(1)5: Using a dedicated line (including virtual dedicated lines of security level equivalent to that of dedicated lines) for connecting the financial company to its subsidiary electronic financial business operator; [Additional Measures]: Identification and secure management of data exchanged between internal systems and cloud systems.	
5	Encryption and Key Management	[Essential Measures]: Article 19: (1) To prevent the distribution and misuse of encryption programs, financial companies or electronic financial service providers shall designate a responsible person for such programs, prohibit unauthorized use by any person other than the responsible person, and store the source program separately. (2) Financial companies or electronic financial service providers must establish	Customers should implement encryption measures for information storage and transmission based on regulatory requirements, and develop and execute a security management plan covering the entire lifecycle of cryptographic keys. 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 Service (KMS), which

No.	Domain	Summary of Controls	Tencent Cloud's Response
		procedures and methods for the injection, operation, renewal, and destruction of keys (including passwords or keys of authentication systems, etc., used to verify the authenticity and integrity of programs) applicable to cryptographic and authentication systems, and manage these keys securely.	provides full lifecycle management.
		Article 19-2: To prevent the leakage of user authentication methods such as passwords and biometric information, financial companies or electronic financial service providers shall establish and implement management measures, including the issuance, safekeeping, periodic renewal, and handling procedures for authentication failures.	<u>Key Management Service (KMS)</u> supports a series of secure operations for keys, including generation, storage, distribution, import, export, use, recovery, archiving, and destruction, to prevent key leakage. The Customer Master Key (CMK) is the core resource in KMS. The CMK serves as the primary key for users, mainly used for data encryption and decryption. Users can utilize KMS's automatic CMK generation feature to create a CMK or form a CMK by importing their own keys. 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.
		Article 34-3(1): A financial company or electronic financial business entity shall keep the passwords of users kept in the information processing system and computer data by encrypting them and prevent them from inquiring the passwords. Provided, That where it is deemed inevitable to inquire a password, the grounds, details, etc. of the inquiry shall be recorded and managed.	<u>CloudAudit</u> service can record operation events related to the Key Management System. Customers can view relevant operation logs by accessing the CloudAudit console.
		Encryption for data storage, transmission, and reception in compliance with laws and regulations, such as the Personal Information Protection Act, the Credit Information Use and Protection Act, and the Act on Promotion of Information and Communications Network	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. Additionally, customers can utilize <u>Virtual Private Cloud (VPC)</u>, <u>Direct Connect (DC)</u>, <u>VPN Connection</u> and other services to achieve secure data transmission in different scenarios. For more information on data transmission security, please refer to number 3 and 4 in Chapter 6.6 of this

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Utilization and Information Protection.	guide.
		[Additional Measures]: Development of a comprehensive management plan throughout the entire key lifecycle considering the possibility of access to key by external parties including cloud service providers.	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. Tencent Cloud also considers factors such as key purpose, sensitivity of protected data, likelihood and impact of compromise to manage keys throughout their lifecycle.
6	Logging	[Essential Measures]: Article 13(1)9: The operation records of the information processing system shall be automatically recorded and maintained by the Director of the Financial Supervisory Service regardless of whether the connection is successful or not and shall be preserved for at least one year. Article 18: Each financial company and electronic financial business operator shall establish and implement appropriate measures, including those related to the address system, allocation, and management, to ensure the secure use of information provider addresses (hereinafter referred to as "IP addresses"), and shall keeping and preserving a separate record that indicates the details of Internet access using his/her or its internal and external IP addresses,	Customers should log and regularly review the operational activities of critical accounts, such as cloud console management accounts. 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 addresses and usernames. Tencent Cloud provides customers with Cloud Log Service (CLS). As an all-in-one log service platform, CLS offers a full range of services including log collection, storage, search and analysis, real-time consumption, and log delivery, assisting customers in addressing issues related to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		for at least one year; Article 25: Each financial company and electronic financial business operator shall regularly conduct an analysis, etc. of the status of use and development of the information processing system in order to prevent system failures and optimize system performance. [Additional Measures]: Logging and regular review of activities on critical accounts, including cloud management console administrator.	business operation, security monitoring, log auditing and log analysis. 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 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.
7	Virtual Environment Security	[Additional Measures]: Regular updates to virtual image templates and periodic reviews of security, including image integrity.	Customers should regularly check the security status of virtual images and ensure that virtual image templates are up to date. Tencent Cloud provides Cloud Virtual Machine (CVM), a scalable virtualized computing service that allows customers to customize resources such as CPU, memory, storage, network, and security. Tencent Cloud offers secure official public images containing licensed operating systems and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud initialization components. CVM also supports creating or importing custom images, as well as sharing and deleting them. To ensure CVM security, customers can configure security groups and network ACLs to define flexible access control policies for hosts and networks, effectively setting firewall rules for different instances. CVM supports sensitive operation protection, requiring identity verification before executing critical actions. Tencent Cloud also offers Cloud Monitoring, which provides real-time alerts and security services such as DDoS protection, DNS hijacking detection, intrusion detection, vulnerability scanning, web trojan detection, and login protection. For container image management, Tencent Cloud Container Registry (TCR) provides secure, dedicated, and high-performance container image hosting and distribution services. Customers can also use Tencent Cloud Container Security Service (TCSS) to protect container and image security. TCSS supports container asset management, image vulnerability scanning, runtime intrusion detection, and security baseline configuration management, enabling full lifecycle protection from image creation and storage to runtime. To strengthen security during virtual machine and virtualization service operations, Tencent Cloud has established virtualization security management standards, defining responsibilities for resource management, access control, and configuration management. Tencent Cloud employs multiple technical measures, including virtual machine isolation and resource control, patch management and

No.	Domain	Summary of Controls	Tencent Cloud's Response
8	Security Monitoring and Vulnerability Analysis and Evaluation	[Essential Measures]: Article 14(1): 1. Create and store each of the following items A. Operating Manual for Major Information Processing Systems B. Director of Maintenance Management who recorded the implementation of regular maintenance for major information processing systems C. Department of Persons Responsible for Information Processing Systems and Disability Situation Registry. Article 14(4): Installing quickly any important patches urgently required in relation to the operating system, utilities, etc. of the information processing system; Article 15(1)1 to 2: 1. Establishing and operating an information protection system to prevent accidents due to any hacking and other electronic trespass; 2. Immediately installing any urgent and important patches related to system programs, etc. to prevent any hacking or other electronic trespass; Article 15(2) to (3): (2) The matters prescribed by the Director of the Financial Supervisory Service shall be observed for the safe operation of the information protection system under paragraph (1) 1.	vulnerability protection, and Hypervisor hardening, to build a robust virtualization security defense system. Customers should set up real-time alerts for major changes within cloud services, implement monitoring, and adopt comprehensive security operations management for key information processing systems. Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. Tencent Cloud also provides customers with the Tencent Cloud Observability Platform (TCOP), which supports users in conducting real-time monitoring, analysis and alerting on cloud products and cloud resources. TCOP collects and displays via visual charts various monitoring metrics automatically reported by cloud products such as Cloud Virtual Machines (CVMs) and cloud databases, as well as those reported based on customers' custom configurations. This helps customers keep real-time track of cloud product resource utilization rates, application performance and the operating status of cloud products. TCOP supports setting up alerts for metrics, and in accordance with the configured alert rules, it promptly notifies customers of business anomalies through means such as message push notifications. Tencent Cloud also provides customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(3) A responsible person shall be designated and managed for the information protection system referred to in any subparagraph of paragraph (1), and the results of operation thereof shall be preserved for at least one year. Article 16: Each financial company and electronic financial business operator shall establish and implement measures to prevent malicious code infections, promptly take necessary measures to minimize the spread of and damage from the malicious code. Article 37-2: (1) Each financial company or electronic financial business operator, the total assets of which are at least two trillion won and the number of regular employees (based on persons from the payment to whom a person obligated to withhold tax under the Income Tax Act collects earned income tax; hereinafter the same shall apply) of which is at least 300, shall conduct analysis and evaluation of weak points in an electronic network for financial transactions at least once a year (for the homepage, at least once a half year). (2) Each financial company and electronic financial business operator shall organize an in-house task force comprised of at least five persons including the chief information security officer (where the chief information security officer does not exist, the chief executive officer shall designate him/her) for analysis and	with a range of related products and services to assist with their security operations, including: • <u>Cloud Security Center (CSC)</u>: As a one-stop security management platform, it helps customers achieve a closed-loop security operation process of pre-event threat detection, in-event response and handling, and post-event traceability analysis through the Asset Center, Risk Center, Alert Center, and Advanced Security Management. CSC supports unified security management of cloud assets, including automated asset inventory, security risk detection and identification, and automated response and handling of security risks. CSC collects threat alerts and logs from Cloud Firewall and Web Application Firewall and uses Tencent Cloud threat intelligence and proprietary security knowledge bases to perform automated data analysis and investigation, providing customers with centralized threat detection, investigation, and response capabilities. • <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. • <u>Cloud Log Service (CLS)</u>: CLS is a

No.	Domain	Summary of Controls	Tencent Cloud's Response
		evaluation of weak points in an electronic network for financial transactions, and at least 30 percent of the constituent members shall be qualified for high quality technical personnel prescribed by the standards for designation of specialized information security service enterprises prescribed in Article 8 of the Enforcement Rule of the Act on the Promotion of Information Security Industry: Provided, That where it entrusts such analysis and evaluation to an institution specialized in evaluation under Article 37-3 (1), it may choose not to organize an in-house task force. (3) A person, other than a financial company or electronic financial business operator under paragraph (1), shall conduct analysis and evaluation of weak points in an electronic network for financial transactions at least once a year (for the homepage, at least once a half year), but may choose not to organize an in-house task force. In such cases, details of analysis and evaluation of weak points shall be prescribed by the Governor of the Financial Supervisory Service. (4) Each financial company and electronic financial business operator may conduct evaluations by dividing facilities subject to evaluation and periods of evaluation. (5) Each financial company and electronic financial business operator shall formulate and execute an implementation plan	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 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. To support customers in complying with regulatory requirements, the Tencent Cloud security team has established a 7x24 security operation system focused on core scenarios such as vulnerability monitoring, intrusion traceability, and attack blocking. It responds to security alerts in real-time, rapidly completes attack source tracing, and formulates emergency response plans to effectively contain the spread of security incidents. For operational changes that may impact customers, Tencent Cloud promptly notifies relevant customers through official channels such as the website and in-site messages.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		according to analysis and evaluation of weak points, and comply with the following matters: 1. Eliminating weak points as a result of analysis and evaluation of weak points or taking actions corresponding thereto; 2. Where it is impracticable to eliminate weak points or take actions corresponding thereto, approval shall be obtained from the chief executive officer; 3. Results of the execution of an implementation plan shall be reported to the chief executive officer. (6) A financial company or electronic financial business entity may request cooperation from subsidiary electronic financial business operators to fulfill the obligations specified in Paragraphs (1) and (3). [Additional Measures]: Real-time monitoring and alerts for major changes in cloud services. [Additional Measures]: For critical information processing systems, apply integrated security controls from an incident response organization.	
9	Personnel Security	[Essential Measures]: Articles 8(1) 2: Securing an in-house organizational structure and personnel to review the appropriateness of contracts for other reserve personnel; [Additional Measures]: Clearly define and manage the responsibilities of cloud service	Customers should identify and manage the permissions and responsibilities of cloud service providers and managed cloud service providers. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		providers and other service providers entrusted with operating cloud services.	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 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". On its international portal, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. In terms of data center operation management, Tencent Cloud has deployed two leased data centers in South Korea. To ensure resilience and security, Tencent Cloud has established a comprehensive management framework covering supplier onboarding, contractual obligations, and ongoing supervision: • Supplier Selection: Tencent Cloud enforces strict security assessment and admission standards, conducting thorough due diligence on physical security, information security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management, and business continuity capabilities to ensure compliance with high security standards. - Contractual Agreements: Tencent Cloud formalizes responsibilities and service boundaries through standardized contracts, clearly defining service scope and quantifying key service standards such as availability levels, thereby ensuring contractual assurance of service quality. - Operational Oversight: Tencent Cloud implements continuous monitoring and evaluation mechanisms, regularly assessing the technical capabilities, service responsiveness, and risk management effectiveness of data center operators. This ensures that any risk management deficiencies of the data center operators do not impact Tencent Cloud's core service delivery capabilities to customers. Furthermore, Tencent Cloud actively cooperates with customers' outsourcing management requirements by providing dedicated personnel to assist and support audits or evaluation activities initiated by customers. It also offers various security protection measures and related cloud products/services to ensure the confidentiality and integrity of customers' cloud data.

6.7 Key Items to Be Included in the Cloud Computing Service Entrustment Agreement

Appendix 2-5 Key Items to Be Included in the Cloud Computing Service Entrustment Agreement sets forth the mandatory provisions to be included in outsourcing contracts signed between financial companies or electronic financial service providers and cloud computing service providers, divided into Basic Items and Additional Items.

- Basic Items include:
 - Overview of tasks and systems associated with the use of the cloud computing service
 - Details of the data to be entrusted for the ordinary course of business
 - Notification obligations for material changes to the entrustment agreement or reentrustment
 - Obligation to allow inspections and access by supervisory authorities or internal/external auditors
 - Cooperation on emergency response training, vulnerability analysis and evaluation, security incident response training, etc.
 - Security controls to be implemented by the cloud computing service provider
 - Security requirements, including information protection obligations and guarantees for service continuity
 - Right to terminate the agreement if the service is likely to be adversely affected
 - Right to monitor compliance with the Service Level Agreement (SLA) and take corrective measures
 - Protection of customer information and maintenance of confidentiality
 - Data destruction at the end of termination of the entrustment agreement
 - Obligation to comply with relevant laws and regulations, and obligation to report compliance
 - Data access control
 - Allocation of responsibilities between the entrusting company and the entrusted company in the event of user harm due to computer incidents, etc.
 - Jurisdiction for litigation of the entrusted company in dispute resolution proceedings
- Additional Items include:
 - Location where information processing—a task entrusted by a financial company—is performed
 - Emergency measures, including data access privileges, in case of service disruptions
 - Obligations to support and plan for transitions when entrusted tasks are transferred to another entity or financial company
 - Procedures and measures for handling major events, such as mergers, splits, changes in contractual status, or re-entrustment
 - Requirement for financial company consent for re-entrustment or changes in reentrustment
 - Cloud computing service provider's obligation to oversee and manage all aspects of re-entrustment

Pursuant to subparagraph 1 of paragraph (1) of Article 14-2 of these Regulations, if the cloud computing service used is classified as a material business, the relevant contract shall include both Basic Items and Additional Items; if classified as a non-material business, only Basic Items shall be required.

As a cloud service provider, Tencent Cloud makes online legal documents available on its international official website, including [Terms of Service](#), [Service Level Agreement \(SLA\)](#), and [Data Processing and Security Agreement](#), which clearly specify the scope and service levels of Tencent Cloud's services, protection of user data and intellectual property rights, security responsibilities and obligations of both customers and Tencent Cloud, service term and agreement termination scenarios, dispute resolution mechanisms, and notification mechanisms. Customers may also choose to sign offline agreements with Tencent Cloud to negotiate and confirm the terms and details thereof.

Cloud services provided by Tencent Cloud to customers are delivered based on the Service Level Agreement (SLA) agreed on each service. Performance indicators, measurement standards, and reporting requirements for each service are clearly defined in the SLA for the respective product and published on Tencent Cloud's official website. Tencent Cloud continuously tracks the performance and availability of its cloud services and provides customers with real-time monitoring via the management console.

Regarding sub-processing scenarios, clauses including prior consent for sub-processing, notification before adding or replacing sub-processors, and data protection obligations are clearly stipulated in agreements such as the [Data Processing and Security Agreement](#). Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the contract/agreement without the customer's prior consent. Tencent Cloud will notify the customer via email or other channels of any intended changes involving the addition or replacement of sub-processors. Meanwhile, for sub-processor management, Tencent Cloud has established a comprehensive supply chain security management system and exercises effective control over suppliers through strict supplier security assessment and onboarding, regular supervision and evaluation, and clear outsourcing service agreements, so as to ensure that sub-processing does not affect Tencent Cloud's ability to provide relevant services to customers, the confidentiality and integrity of customer information processing, or the supervision and audit rights of customers or relevant regulatory authorities. In addition, Tencent Cloud will actively cooperate with customers' outsourcing management requirements and respond to and participate in audit or assessment activities initiated by customers.

In terms of compliance and data sovereignty, Tencent Cloud has established a comprehensive internal information security and privacy protection management system and strictly complies with laws and regulations relating to cybersecurity, user privacy, and data security in the jurisdictions where it operates. Tencent Cloud adheres to the principle of data confidentiality — internal employees of Tencent Cloud will never proactively access any customer data unless required for service provision or troubleshooting, with the customer's explicit authorization, or in compliance with national laws and regulations such as investigations into criminal cases by national or local government authorities. If disclosure of customer data is required by mandatory legal provisions, Tencent Cloud will comply with relevant legal requirements and promptly notify the customer. Meanwhile, Tencent Cloud implements full-node real-name verification and management for data access rights to safeguard the integrity of data assets and the reliability of business services, and has established real-time monitoring and blocking mechanisms to detect and prevent any

abnormal data access behaviors. Furthermore, Tencent Cloud upholds the principle of openness and transparency; if customers require information such as the location of data storage, Tencent Cloud will promptly provide such information through appropriate channels.

In terms of business continuity and emergency response, Tencent Cloud builds or leases data centers in multiple regions around the world in accordance with relevant international standards and local security requirements, providing customers with a choice of multiple regions and availability zones, while strictly complying with laws and regulations relating to user privacy and data security protection in the jurisdictions where it operates, and continuously and proactively monitoring local regulatory developments. Currently, Tencent Cloud operates two data centers in South Korea, providing a wide range of cloud computing services including Cloud Virtual Machine (CVM), Cloud Database, and Cloud Storage. Customers may independently and flexibly deploy their data and systems in different regions or availability zones according to business development needs and data security requirements. Meanwhile, Tencent Cloud's various cloud products and services — including computing services, network services, storage services, database services, container and middleware services, and security services — are all highly available and equipped with corresponding disaster recovery and resumption plans. Tencent Cloud has also established a comprehensive internal business continuity management system and has obtained the international standard certification of ISO/IEC 22301 for Business Continuity Management Systems.

Regarding incident reporting, Tencent Cloud has formulated information security incident management specifications and established relevant procedures for information security incident response, escalation and notification, so as to provide early warnings or notifications to internal personnel, customers and other relevant parties that may be or have been affected by incidents in a timely manner, ensuring orderly, timely and efficient communication and coordination among all parties. For security incidents that may affect customers, Tencent Cloud will, after internal evaluation based on the scope and severity of the information security incident, notify customers of the handling and analysis results of the information security incident through appropriate channels and provide corresponding technical support to assist customers in taking remedial measures to minimize losses.

To support customers' audit and review requirements, Tencent Cloud provides dedicated personnel to actively cooperate with audit or review activities initiated by customers.

Meanwhile, Tencent Cloud's security team conducts internal security audits at least once a year and continuously monitors the status of the cloud platform and internal systems to maintain a sound security posture and comply with relevant laws, regulations and security management standards. Tencent Cloud also undergoes regular professional audits and assessments by independent third parties. To date, Tencent Cloud has obtained a number of security and privacy compliance certifications and qualifications through independent third-party audits or assessments. Based on customer needs, Tencent Cloud also provides assurance-based System and Organization Controls (SOC) reports to disclose its latest internal control over service organizations to cloud user organizations, independent auditors, regulators, shareholders and other relevant stakeholders.

If customers need to terminate the contract or agreement due to business changes or future IT planning, they may choose to back up and migrate their cloud data and production environments at any time. Tencent Cloud supports customers in backing up or migrating data using common standard formats, allowing customers to use the same transmission methods

and protocols as during cloud onboarding, or network service products such as [Direct Connect \(DC\)](#) and [VPN Connection](#), to ensure secure and reliable data migration during termination of cloud service engagement. Upon service termination by customers, Tencent Cloud will following strict data erasure methods, permanently delete customer data including replicas and backups upon expiration of the retention period, and such deleted data cannot be recovered.

07

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Regulation on Entrustment, etc. of Duties by Financial Institutions

Regulation on Entrustment, etc. of Duties by Financial Institutions specify the management requirements that financial companies shall comply with when outsourcing businesses for which they have obtained authorization, approval or registration pursuant to Article 17(3) of the Act on the Establishment of the Financial Services Commission.

In this chapter, Tencent Cloud will extract and summarize the control requirements relevant to cloud service providers under the Regulation on Entrustment, etc. of Duties by Financial Institutions, and describe how Tencent Cloud, as a cloud service provider, assists financial companies in complying with such requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3	Entrustment, etc. of Duties	(1) In performing duties the authorization, etc. for which are obtained, a financial institution may entrust the duties to a third party or receive entrustment of duties from a third party. (3) Where a financial institution entrusts duties to a third party or receives entrustment of duties from a third party pursuant to paragraph (1), it shall have the duties implemented properly in consideration of the following: 1. Expense-benefit analysis with regard to entrustment of duties or receiving entrustment of duties; 2. Whether damage occurs to financial customers or the financial order is disrupted; 3. Whether a third party can be entrusted with duties pursuant to relevant laws (Provided, That where a third party is a foreigner, pursuant to Article 3 of the Act on Private International Law); 4. Whether a third party is able to properly implement duties entrusted to him/her; 5. Whether relevant statutes, such as the Act on Real Name Financial Transactions and Confidentiality, are violated.	Customers should comprehensively consider the capabilities and qualifications of third parties, the impact of the delegation on financial consumers and financial order, as well as relevant regulatory requirements when commissioning or being commissioned, to ensure appropriate handling of the business. Customers should also clarify their own responsibilities in delegation scenarios. 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 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 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. Recognizing that

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(4) A person who is entrusted with duties from a financial institution pursuant to paragraph (1) may re-entrust the duties to a third party with the approval of the entrustor. In such cases, Article 2, paragraphs (1) through (3) of this Article, and Articles 4 through 6 shall apply mutatis mutandis, and the financial institution originally entrusted with the duties shall make a report after re-entrustment. (5) Where duties are entrusted pursuant to paragraph (1) (including cases in which duties are re-entrusted pursuant to paragraph (4)), the entrusting company shall be jointly and severally responsible together with the entrusted company for the compensation for damage occurring from the violation of finance-related statutes, such as these Regulations, and of obligations under the standard for conferring or receiving entrustment of duties under Article 3-2.	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". In terms of capability and scale, as a cloud computing brand under Tencent, a leading enterprise in China's internet industry, Tencent Cloud's operational capacity and scale are among the leaders in the industry. Tencent Cloud has obtained multiple professional certifications from industry organizations. Its data centers span multiple regions worldwide, including Mainland China, Asia-Pacific, North America, and Europe. Tencent Cloud has partnered with over 11,000 companies and delivered more than 400 industry solutions across 30+ sectors. In terms of compliance, 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 conducts annual security testing, risk assessments, and internal audits of its information systems to maintain a robust security posture in line with relevant security management requirements. Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. For subcontracting scenarios, 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. . For subcontractor 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 to ensure that sub-processing does not impair its ability to provide the relevant services to customers, the confidentiality and integrity of customer information handling, or the supervisory and audit rights of relevant regulatory bodies and financial institutions. In

No.	Domain	Summary of Controls	Tencent Cloud's Response
			addition, Tencent Cloud actively cooperates with customers' outsourcing-management requirements and responds to and participates in audits or assessments initiated by customers.

08

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Regulation on Outsourcing of Data Processing of Financial Companies

Regulation on Outsourcing of Data Processing of Financial Companies specifies the management requirements that financial companies shall comply with when outsourcing information processing business in the course of conducting financial businesses for which they have obtained authorization, approval, registration or other qualifications pursuant to Article 17(3) of the Act on the Establishment of the Financial Services Commission.

In this chapter, Tencent Cloud will extract and summarize the control requirements relevant to cloud service providers under the Regulation on Outsourcing of Data Processing of Financial Companies, and describe how Tencent Cloud, as a cloud service provider, assists financial companies in complying with such requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
4	Entrustment of Information Processing	(1) A financial company may entrust the information processing to a third party if the information processing is required to conduct the business for which it is licensed, etc. (2) Notwithstanding the provisions of paragraph (1), the information processing shall not be entrusted in any of the following cases: Provided, That in the following subparagraph 2, the entrustment of the management of ledgers, etc., to Koscom or the Korea Federation of Savings Banks in the manner permitted by the Governor of the Financial Supervisory Service shall be excluded: 1. Where applicable laws prohibit the entrustment of information processing; 2. Where institutional warnings or higher, or criminal penalties have been received at least twice within the last three years because of matters related to the inspection of the supervisory authority, such as the management of financial user information or submission of supervision-related materials; 3. Where the entrustment of information processing	When customers delegate information processing business to a third party and enter into an information processing delegation agreement, the contract must explicitly specify data access controls, the division of responsibilities between the parties in the event of user harm due to incidents such as computer-related issues, the delegate's obligation to accept inspections and audits by regulatory authorities, and the jurisdiction of the courts in dispute resolution proceedings, among other matters. The delegate, in turn, should process the received information within the scope of the original delegation, equip the necessary computer facilities and personnel that meet the requirements, and ensure compliance with the same standards in scenarios involving further delegation. 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 agreements may be terminated. Customers may also choose to enter into an

No.	Domain	Summary of Controls	Tencent Cloud's Response
		significantly undermines the soundness or credibility of a financial company, or if there is a serious concern that financial order may be disrupted or financial users may suffer damage. (3) When entering into an information processing entrustment agreement pursuant to paragraph (1), a financial company shall clarify the liability relationship that may arise from the entrustment by including in the contract the control of access to data, liability relationship between the company and the entrusted company for user damage caused by computer incidents, the obligation of the entrusted company to accept supervision and inspection by the supervisory authority, and the jurisdiction of the court in the dispute resolution process of the entrusted company. (4) An entity entrusted with the information processing pursuant to paragraph (1) may reentrust the tasks to a third party. In this case, paragraphs (2), (3), (5), and (6) of this Article and Articles 5, 7, and 8 shall apply mutatis mutandis. (5) The person entrusted with the information processing pursuant to paragraph (1) shall not use the information obtained during the process of the information processing for any other purpose beyond the scope of the entrustment agreement: Provided, That the consent of the information subject is obtained, the information	offline agreement with Tencent Cloud to negotiate specific terms and conditions. In terms of compliance and data sovereignty, Tencent Cloud has established a comprehensive information security and privacy protection management system and strictly complies with cybersecurity, user privacy, and data protection laws and regulations in the jurisdictions where it operates. Adhering to the principle of “data confidentiality,” 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). Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent any abnormal data access activities. In terms of human resources, Tencent has established specialized security teams across different functions and domains, supported by an experienced industry expert service team dedicated to delivering secure, reliable, professional, and compliant products and services. Regarding sub-processing scenarios, clauses including prior consent for sub-processing, notification before adding or replacing sub-processors, and data protection obligations are clearly stipulated in agreements such as the Data Processing and Security Agreement. Tencent Cloud will not sub-contract any processing activities performed on behalf of the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		may be used within the scope of the consent. (6) In the case of entrusting information processing pursuant to paragraph (1), the computer facilities and personnel related to the entrusted processing shall be considered in determining whether the requirements for obtaining computer facilities and personnel for licensing under relevant laws and regulations are met. (7) In the case of entrusting information processing pursuant to paragraph (1) (including reentrusting pursuant to paragraph (4)), the entrusting company shall be jointly and severally liable with the entrusted company for damages to the information subject and users caused by the entrusted company's violation of its obligations under these Regulations, related laws, and the entrustment agreement pursuant to paragraph (3).	customer under the contract/agreement without the customer's prior consent. Tencent Cloud will notify the customer via email or other channels of any intended changes involving the addition or replacement of sub-processors. For sub-processor management, Tencent Cloud has established a comprehensive supply chain security management system and exercises effective control over suppliers through strict supplier security assessment and onboarding, regular supervision and evaluation, and clear outsourcing service agreements, so as to ensure that sub-processing does not affect Tencent Cloud's ability to provide relevant services to customers, the confidentiality and integrity of customer information processing, or the supervision and audit rights of customers or relevant regulatory authorities. In addition, Tencent Cloud will actively cooperate with customers' outsourcing management requirements and respond to and participate in audit or assessment activities initiated by customers.
5	Protection of Specific Information	(1) In case of entrusting information processing under Article 4, a financial company shall faithfully implement measures to secure safety prescribed in each relevant law. In this case, the identifiable information of individual customers shall be protected by encryption and other measures and, in particular, shall not be transferred overseas. (2) A financial company shall disclose concrete details of safety measures taken to protect entrusted	When delegating information processing, customers should implement security safeguards in accordance with relevant regulatory requirements (including encryption of personally identifiable information and restrictions on its transfer abroad, among others) and disclose the security measures taken through channels such as websites. For the processing of sensitive information, customers should additionally provide separate notifications to the data subjects. For data storage protection, Tencent Cloud's storage and database products support data encryption using secure, high-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		processed information through its website, etc. In addition, in the case of entrusting the processing of sensitive information to a third party, the information subjects shall be informed in the manner determined by the Governor of the Financial Supervisory Service.	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. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. To meet Customer requirements for business continuity and data localization, Tencent Cloud builds or leases data centers in multiple global locations in accordance

No.	Domain	Summary of Controls	Tencent Cloud's Response
			with relevant international standards and local security requirements. Tencent Cloud strictly complies with applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Currently, Tencent Cloud operates two data centers in South Korea, providing a variety of cloud computing services including Cloud Virtual Machines (CVM), Cloud Databases, and CDN. South Korean customers can choose to store and process their data locally in South Korea. For more information on the collection, processing, and sharing of personal information by Tencent Cloud, please refer to the Privacy Policy. 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, 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. Moreover, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
7	Reporting	(1) If a financial company intends to entrust the processing of the financial transaction information of individual customers as referred to in Article 4(1) (with the exception of cases where the content of the financial transactions cannot be identified) and if the entrusted entity is located outside the country, the entrusted entity shall report the matter to the Governor of the Financial Supervisory Service by attaching the following documents thirty (30) business days before the day when the entrusted tasks are to be performed: 1. A copy of the entrustment agreement (draft); 2. "Business entrustment operation standards" to be prepared and observed by financial institutions pursuant to Article 3-2 of the Regulations on Business Entrustment, etc. of Financial Institutions; 3. A copy of the opinion of the compliance officer (in the absence of a compliance officer: an equivalent person, such as an auditor) and related materials proving that the business entrustment agreement does not violate relevant laws, including these Regulations;	Customers should ensure that the delegate submits applicable materials to the Financial Supervisory Service within the stipulated timeframe as required by the regulations and cooperates with the supervision and inspections conducted by the Financial Supervisory Service. 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. 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. 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. For issues identified or suggestions raised by customers or relevant regulatory bodies, Tencent Cloud will assess their potential impact on customers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		4. Purpose and expectations of entrustment; 5. Major changes in business execution procedures due to entrustment; 6. Documents proving the ability of the supervisory authority to supervise the operation of information processing that has been entrusted; 7. Information about the other party to the entrustment agreement (including the other party to the reentrustment agreement if reentrustment is planned) (name, capital size, location, main business, and, in the case of an individual, the name of the representative) 8. Procedure to relieve victims in the event of computer incidents and information leakage; (2) If a financial company intends to entrust the processing of the financial transaction information of individual customers as referred to in Article 4(1) (with the exception of cases where the content of the financial transactions cannot be identified) and if the entrusted entity is located in the country, the entrusted entity shall report the matter to the Governor of the Financial Supervisory Service by attaching the documents prescribed in paragraph (1) seven (7) business days before the day when the entrusted tasks are to be performed.	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. Regarding incident response and handling, 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 handle the incidents. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(3) If a financial company intends to entrust the processing of financial transaction information other than financial transaction information subject to reporting required under paragraphs (1) and (2), the entrusted entity shall report the matter to the Governor of the Financial Supervisory Service by attaching documents listed in paragraph (1) within ten (10) business days from the day when the entrusted tasks are to be performed.	minimize losses.
8	Supervision and Inspection	(1) Entrusting financial companies and entrusted companies shall accommodate the requests for supervision and inspection, including the submission of materials to the Governor of the Financial Supervisory Service, in relation to information processing tasks entrusted under Article 4.	

09

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 Commission (FSC) of South Korea, 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.

10

Version History

Date	Version	Detail