Tencent Cloud

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

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

Tencent Cloud

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

Service Statement

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

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

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

CONTENTS

01 Overview

02 Tencent Cloud Security and Privacy Compliance

2.1 Global Compliance 4
2.2 ISO/IEC Certification 4
2.3 Regional and Industry Compliance 6

03 Tencent Cloud Security Responsibility Sharing Model

04 Tencent Cloud Global Infrastructure

05 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Notice 658: Management of Outsourced Relevant Services for Banks and Notice 1121: Management of Outsourced Relevant Services for Merchant Banks

5.1 Requirement of Material Ongoing Outsourced Relevant Services 17
5.2 Requirements for Outsourcing Relevant Services Involving Customer Information 28

06 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Notice on Cyber Hygiene

07 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Technology Risk Management Guidelines

7.1 Technology Risk Governance and Oversight 44
7.2 Technology Risk Management Framework 48
7.3 IT Project Management and Security-by-Design 50
7.4 System Development Life Cycle and Security-By-Design 55
7.5 IT Service Management 60
7.6 IT Resilience 67
7.7 Access Control 76
7.8 Cryptography 81
7.9 Data and Infrastructure Security 84
7.10 Cyber Security Operations 92
7.11 Cyber Security Assessment 95
7.12 IT Audit 98

08 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions other than Banks)

09 How Tencent Cloud Meets and Assists

CONTENTS

Customers to Meet the Requirements of Guidelines on Business Continuity Management

10 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption

11 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Control Objectives and Procedures for Outsourced Service Providers

11.1 Audit and Inspection of Technology Risk Governance and Oversight 159
11.2 Physical Security 161
11.3 General Information Technology Controls 166
11.4 Service Level Controls 178

12 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Cloud Computing Implementation Guide

12.1 Cloud Risk Assessment & Due Diligence 182
12.2 Key Controls Recommended when Entering into a Cloud Outsourcing Arrangement 189

13 Conclusion

14 Version History

01 Overview



In recent years, the technological landscape of the financial industry has been evolving rapidly, with many financial institutions actively embracing digital transformation to enhance operational efficiency and deliver superior financial services to consumers. However, digital transformation also exposes financial institutions to increasingly diverse technology risks. To help institutions recognize technology and cybersecurity risks and adopt effective mitigation measures, the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) have issued a series of regulatory notices, guidelines, and advisories. These cover areas such as cybersecurity, technology risk management, business continuity planning, outsourcing arrangements, and cloud adoption, providing clear guidance to standardize operational practices, strengthen cyber resilience, and ensure the security and stability of technology applications.

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

Monetary Authority of Singapore (MAS):

- Notice 658: Management of Outsourced Relevant Services for Banks
- Notice 1121: Management of Outsourced Relevant Services for Merchant Banks
- Notice on Cyber Hygiene
- Technology Risk Management Guidelines
- Guidelines on Outsourcing (Banks)
- Guidelines on Outsourcing (Financial Institutions other than Banks)
- Business Continuity Management Guidelines
- Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption

Association of Banks in Singapore (ABS):

- Guidelines on Control Objectives and Procedures for Outsourced Service Providers
- Cloud Computing Implementation Guide

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) financial industry	The Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), and Insurance Authority (HKIA) have issued key regulatory requirements to govern the use of information technology by financial, insurance, and securities institutions. Tencent Cloud has successfully undergone independent third-party audits, demonstrating that it is a trusted cloud service provider for the financial industry. By taking a proactive approach to fulfilling strict compliance obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure.
IT compliance audit in	Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange

Thailand financial industry	Commission (OSEC), the Office of Insurance Commission (OIC), and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's compliance with Thailand's stringent financial industry regulatory requirements and its commitment to providing high-quality, compliant cloud services to financial sector customers.
IT compliance audit in Indonesian financial industry	Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan, OJK), and other Indonesian financial regulatory authorities have issued regulations for the financial services industry. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits confirm that Tencent Cloud strictly complies with the regulatory requirements of Indonesia's financial industry when providing cloud services to financial customers.
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 organisations 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 and 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	
	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	Shared Responsibilities
	Cloud Application Security	Cloud Application Security	Cloud Application Security	
	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	Tencent Cloud Responsibilities
	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	
	Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security	

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

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

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

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

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

For more information about the responsibility sharing model, please refer to the Tencent Cloud Security White Paper.

04 Tencent Cloud Global Infrastructure



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

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

Tencent Cloud currently operates over 2,300 acceleration nodes in Mainland China, covering multiple carriers, and more than 900 acceleration nodes overseas across 70+ countries and regions. By distributing content to global acceleration nodes and leveraging a global scheduling system, users can access content from the nearest node, reducing latency.

Tencent Cloud also enhances data isolation and security through independent sites and technologies such as data encryption, access control, and audit tracking, preventing data leakage and unauthorized access while strengthening regional isolation and compliance.

For more information about Tencent Cloud infrastructure, please refer to Tencent Cloud Global Infrastructure.

05

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Notice 658: Management of Outsourced Relevant Services for Banks and Notice 1121: Management of Outsourced Relevant Services for Merchant Banks

On December 11, 2023, the Monetary Authority of Singapore (MAS) issued Notice 658: Management of Outsourced Relevant Services for Banks and Notice 1121: Management of Outsourced Relevant Services for Merchant Banks, which set out the requirements that Singapore banks1 and merchant banks2 must comply with when outsourcing relevant services to manage associated risks. The provisions of these two notices are largely consistent, focusing primarily on areas such as material ongoing outsourced services and outsourced services involving the disclosure of customer information.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in Notice 658 and Notice 1121, and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in complying with these requirements.

5.1 Requirement of Material Ongoing Outsourced Relevant Services

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.1	Management of Material Ongoing Outsourced Relevant Services	A bank in Singapore must: (a) implement policies and procedures to identify all material ongoing outsourced relevant services, and assess, manage and monitor any risk to the bank that may arise from obtaining or receiving each of these relevant services; (b) maintain effective supervision and monitor the provision of the material ongoing outsourced relevant service, including establishing appropriate levels of approving authorities that is commensurate with the scale and complexity of the material ongoing outsourced relevant service, to approve matters relating to the relevant service;	Customers must implement policies and procedures to identify all material ongoing outsourced services, assess, manage, and monitor associated risks, establish measures for service termination, and maintain proper documentation. **To support customers' outsourcing oversight and risk management requirements**, Tencent Cloud provides the **Tencent Cloud's Observability Platform (TCOP)**, which enables real-time monitoring, analysis, and alerting for cloud products and resources. TCOP collects monitoring metrics reported by Tencent Cloud services and customer-defined configurations, presenting them through visual dashboards to help customers track the operational status and performance of cloud products. It also supports alert configuration based on defined thresholds and sends notifications via message push and other channels to promptly inform customers of business anomalies. In addition, Tencent Cloud, in accordance with contractual agreements, grants customers audit and oversight rights and provides dedicated personnel to

1 Singapore Bank: "Bank" refers to any company holding a valid banking license under Section 7 or Section 79 of the Banking Act. "Singapore Bank" refers to a bank incorporated in Singapore, or a branch or office located in Singapore of a bank incorporated outside Singapore.

2 Singapore Merchant Bank: "Merchant Bank" refers to any company holding a valid merchant banking license granted under Section 55S of the Banking Act, or deemed to have obtained such license under Section 64. "Singapore Merchant Bank" refers to a merchant bank incorporated in Singapore, or a branch or office located in Singapore of a merchant bank incorporated, formed, or established outside Singapore.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(c) establish measures to minimize any disruption to the operations of the bank in the event that the service provider cannot adequately provide the material ongoing outsourced relevant service or where the bank needs to exercise its right to terminate the outsourcing agreement or to stop obtaining or receiving the material ongoing outsourced relevant service; (d) implement the measures mentioned in sub-paragraph (c) in the event that the service provider cannot adequately provide the material ongoing outsourced relevant service or where the bank needs to exercise its right to terminate the outsourcing agreement or to stop obtaining or receiving the material ongoing outsourced relevant service; and (e) keep documentation sufficient to demonstrate compliance by the bank with the requirements in this paragraph.	actively support customer-initiated audits or inspections. Tencent Cloud also undergoes regular independent third-party audits and publishes System and Organization Controls (SOC) reports to provide assurance on its internal control environment to cloud users, independent auditors, regulators, shareholders, and other stakeholders. **If termination of the agreement is required due to business changes or future IT planning**, backup and migration of cloud data and production environments can be performed at any time. Tencent Cloud supports the use of standard formats for data backup or migration, enabling adoption of the same transmission methods and protocols used during cloud onboarding, or use of network services such as **Direct Connect (DC)** and **VPN Connection**, to ensure secure and reliable data transfer during termination of cloud service engagement.
5.1-5.2	Evaluation of Service Provider for Material Ongoing Outsourced Relevant Services	5.1 Before obtaining any material ongoing outsourced relevant service, a bank in Singapore must establish a framework for evaluating the ability of the service provider to perform the acts mentioned in section the Act, as the case may be. The bank must conduct due diligence checks against the framework and be satisfied of the results. The bank must	Before engaging any material ongoing outsourced service, customers must establish an assessment framework and conduct periodic due diligence in accordance with that framework to ensure that the service provider meets the requirements under the Act. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. Below is an

No.	Domain	Summary of Controls	Tencent Cloud's Response
		ensure that the framework includes an assessment of all of the following matters at the minimum: (a)in the case where the service provider is an intragroup entity of the bank in Singapore, the service provider's risk management framework, and its track record in providing similar relevant services; (b) in all other cases other than that mentioned in paragraph (a), – (i) the service provider's risk management framework; (ii) the service provider's reputation and track record in providing similar relevant services; and (iii) the service provider's financial strength and resources; (c) in the case where the material ongoing outsourced relevant service is obtained or received outside Singapore by the bank and involves the disclosure of customer information to the service provider, – (i) the risks of the bank not being able to comply with any obligations under any written law that requires it to keep confidential, any of its customer information; (ii) the service provider's reputation and track record for safeguarding the confidentiality and integrity of customer information in its custody; (iii) the service provider's ability to ensure that employees who are authorized	overview of Tencent Cloud's capabilities in various aspects of due diligence as a cloud service provider: • **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. • **Financial Strength:**Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant. • **Risk Management:** Tencent Cloud develops and maintains an internal risk management framework based on the **ISO/IEC 27001:2022** standard to identify, analyze, and manage recognized risks. Tencent Cloud conducts a formal risk assessment at least annually, referencing sources such as industry security incident reports, Tencent Cloud's accumulated practices, and professional risk databases. Risks within Tencent Cloud's products and service processes are identified and evaluated based on asset value, likelihood, and impact severity, resulting in a calculated risk level. Based on the risk analysis, Tencent Cloud formulates mitigation strategies and implements corresponding measures to reduce risks to an acceptable level. • **Operational Capacity and Scale:** Tencent Cloud's operational capacity and scale are among the leaders in the industry. Its data centers span multiple regions worldwide, including

No.	Domain	Summary of Controls	Tencent Cloud's Response
		to access the customer information are subject to confidentiality obligations; and (iv) the measures that the service provider has put in place to safeguard the confidentiality and integrity of customer information of the bank that is in the custody of the service provider, in relation to the provision of the relevant service. 5.2 A bank in Singapore must satisfy itself, on an ongoing basis, of the service provider's ability to perform the acts mentioned in the Act, as the case may be. The bank must, at the minimum: (a) after performing the initial due diligence checks mentioned in paragraph 5.1, perform the same due diligence checks within a period assessed by the bank to be commensurate with the risks of the material ongoing outsourced relevant service, but no later than 24 months of obtaining the material ongoing outsourced relevant service; and (b) thereafter, perform the due diligence checks mentioned in paragraph 5.1 at a frequency approved by the board of the bank that is commensurate with the risks of the material ongoing outsourced relevant service.	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. • **Confidentiality Obligation:** Tencent Cloud strictly adheres to laws and regulations governing user privacy and data security in all jurisdictions where it operates. It provides online legal documents such as **Terms of Service**, **Data Processing and Security Agreement**, which clearly define the protection of Customer data, intellectual property, and confidentiality obligations. Tencent Cloud requires internal employees to sign confidentiality undertakings that clearly define confidentiality obligations, while external personnel are bound by confidentiality clauses stipulated in agreements between Tencent Cloud and outsourcing vendors. • **Protection of Information Confidentiality and Integrity**: Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data content. Adhering to the principle of "data privacy," Tencent Cloud employs multi-layered technical isolation measures—such as virtualization control layer access policies, internal private network isolation strategies, web console permission allocation and identity authentication, session IDs and access keys—to ensure data segregation and prevent tenants from accessing, obtaining, or tampering with other tenants' data. Tencent Cloud's storage and database products support data encryption using strong, secure algorithms, integrated with the **Key Management Service (KMS)** for full lifecycle key management, ensuring data confidentiality.

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.3	Requirements relating to Use of Sub-Contractor for Material Ongoing Outsourced Relevant Services	A bank in Singapore must allow a material ongoing outsourced relevant service to be sub-contracted: (a) ensure that the service provider notifies the bank in writing prior to or within a reasonable time of the engagement of a sub-contractor unless the bank's agreement for the engagement of the sub-contractor had been obtained prior to the sub-contractor's engagement; (b) ensure that prior to obtaining or receiving any material ongoing outsourced relevant service, the bank documents its assessment that allowing the subcontracting arrangement for the material ongoing outsourced relevant service, or any part of it, – (i) would not pose any risks to the bank which it is not prepared, or is unable, to manage, in particular, legal, reputational, technological and operational risks; and (ii) would not compromise: (A) the provision of the relevant service to the bank; and (B) the confidentiality and integrity of all information disclosed to, or accessed, collected, copied, modified, used, stored or processed by, the service provider or the sub-contractor, as the case may be, in accordance with the outsourcing agreement and subcontracting arrangement	Customers should maintain control over subcontracting of material ongoing outsourced relevant services, including understanding and reviewing the service provider's subcontracting arrangements and conducting regular assessments of both the service provider and its subcontractors. 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 the Monetary Authority of Singapore and financial institutions. In addition, Tencent Cloud actively cooperates with customers' outsourcing-management requirements and responds to and participates in audits or assessments initiated by customers.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		respectively; (c) ensure that the bank regularly reviews its assessment in paragraph (b), and documents any changes to its assessment, including the reasons for the changes.	
7.1-7.2	Outsourcing Agreement and Access to Information relating to Material Ongoing Outsourced Relevant Services	7.1 Before obtaining a material ongoing outsourced relevant service, a bank in Singapore must enter into an outsourcing agreement that contains terms which achieve the same effect as all of the following: (a) a requirement that the service provider protects the confidentiality and integrity of all information of the bank in its custody, in relation to the provision of the material ongoing outsourced relevant service; (b) a requirement that the service provider ensures that it and its employees only access, collect, copy, modify, use, store or process any customer information of the bank to the extent that is necessary for it and its employees to provide the material ongoing outsourced relevant service; (c) a requirement that the service provider ensures that it and its employees do not disclose any customer information of the bank to any third party unless compelled by law, in which case the service provider must notify the bank as soon as practicable to the extent permitted by law;	Before obtaining material ongoing outsourced relevant services, customers must enter into an outsourcing agreement with the service provider. The agreement should include clauses related to information confidentiality and integrity, restrictions on employee access to customer information, restrictions on employee disclosure of customer information, audit rights of banks and relevant regulators, rights to obtain service-related information, service termination, and data deletion after termination. 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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(d) a requirement that the Authority, or an auditor appointed by the Authority, be allowed to audit the books, systems and premises of the service provider for the purposes of determining whether the service provider is properly providing the material ongoing outsourced relevant service; (e) a requirement that the service provider, on a request by the bank, provides to the bank or the Authority, or any person appointed by the bank or the Authority, any record, document, report or information relating to the provision of the material ongoing outsourced relevant service; (f) a requirement that if the bank terminates the outsourcing agreement or stops receiving the material ongoing outsourced relevant service provided by the service provider, the service provider ensures that all customer information given to the service provider are deleted, destroyed or rendered unusable as soon as possible; and (g) a requirement that the bank may terminate the outsourcing agreement or stop receiving the material ongoing outsourced relevant service from the service provider under any of the following circumstances: (i) by giving reasonable notice to	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. 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 data integrity and service reliability, and has implemented real-time monitoring and interception mechanisms to detect and prevent any abnormal data access activities. **To ensure employees fulfil confidentiality obligations**, Tencent Cloud requires internal staff to sign confidentiality agreements specifying their obligations and responsibilities, as well as potential penalties for violations. Outsourced personnel must undergo background checks prior to employment and comply with confidentiality requirements stipulated in agreements between Tencent Cloud and subcontractors. Confidentiality requirements for employees and third parties are reviewed and updated by Tencent Cloud's legal department as needed. Tencent Cloud also conducts diverse training programs and communicates its personal information and privacy protection policies, processes, and standards through multiple channels

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the service provider; (ii) if directed by MAS to terminate the outsourcing agreement or to stop receiving the material ongoing outsourced relevant service from the service provider; (iii) if the service provider or a sub-contractor, where applicable, has failed to safeguard the confidentiality or integrity of customer information of the bank that is in the custody of the service provider or sub-contractor, where applicable, in relation to the provision of the material ongoing outsourced relevant service; (iv) if there has been a demonstrable deterioration in the ability of the service provider or a sub-contractor, where applicable, to safeguard the confidentiality or integrity of the customer information in its custody. 7.2 Where an intragroup entity of the bank in Singapore has entered into an outsourcing agreement on behalf of the bank, the bank must ensure that the terms set out in paragraph 7.1 are included in the outsourcing agreement before obtaining or receiving the material ongoing outsourced relevant service.	to ensure employees understand their responsibility to protect user data privacy, the disciplinary consequences of violations, and acquire the necessary skills to implement data protection. **Upon service termination**, Tencent Cloud applies strict data erasure procedures. After the retention period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable. If any media used to provide Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud will promptly perform complete physical destruction in accordance with rigorous internal processes. Upon customer request, Tencent Cloud will actively cooperate by providing information to facilitate due diligence or to provide records, documents, reports, or information related to the material ongoing outsourced relevant services to MAS or its designated personnel.
8.1	Protection of Customer Information relating to Material Ongoing	A bank in Singapore that receives a material ongoing outsourced relevant service from a service provider must implement adequate measures to protect customer information	Customers should take appropriate measures to protect customer information disclosed to service providers or subcontractors. This includes providing written notice to the service provider regarding both parties' legal obligations to maintain confidentiality of customer information, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Outsourced Relevant Services	that is disclosed to the service provider or sub-contractor, as the case may be, against unauthorized disclosure, access, collection, copying, modification, use, disposal or similar risks. The bank must at the minimum ensure that the measures include all of the following: (a) notifying the service provider in writing of – (i) the bank's obligation to keep customer information confidential under the Act and common law; (ii) the service provider's obligation to keep customer information confidential under the Act; and (iii) in the case where the material ongoing outsourced relevant service is to be performed outside Singapore, the bank's obligations to protect customer information in accordance with the laws of the place where the material ongoing outsourced relevant service is to be performed; (b) ensuring that customer information is disclosed to, or accessed, collected, copied, modified, used, stored or processed by, a service provider and its employees or a sub-contractor and its employees only to the extent that is necessary for the service provider or the sub-contractor, and their respective employees, as the case may be, to provide the material ongoing	ensuring that the service provider/subcontractor and their employees access or process customer information only to the extent necessary for delivering material ongoing outsourced relevant services. Tencent Cloud strictly complies with privacy and data protection laws and regulations in the jurisdictions where it operates. Tencent Cloud provides online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, which clearly define the protection of user data and intellectual property, as well as confidentiality obligations. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents). **To ensure employees access or process customer information only within the scope necessary for service delivery**, Tencent Cloud has established authorization policies and mechanisms, Permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights. Tencent Cloud enforces strict internal network isolation rules, achieving complete separation between its internal office network and the production environment where customer data resides through physical and logical isolation. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		outsourced relevant service.	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. With respect to sub-contractor management, Tencent Cloud enters into formal service agreements with its sub-contractors that explicitly set out responsibilities and obligations relating to security, privacy protection, confidentiality, and compliance. In addition, Tencent Cloud continuously monitors sub-contractors' service levels to ensure that sub-processing operations remain secure and stable. In accordance with the security and operational standards stipulated in the contracts, Tencent Cloud regularly assesses sub-contractors' delivery performance and takes appropriate remedial action for any issues identified, thereby ensuring that their deliverables meet the agreed security and quality requirements.
9.1	Audit of Material Ongoing Outsourced Relevant Services	A bank in Singapore must conduct independent audits on each of its material ongoing outsourced relevant services, for the purposes mentioned in paragraph 7.1(d) at least once every three years.	Customers should conduct an independent audit of each material ongoing outsourced relevant services at least once every three years. To support customers' outsourcing oversight requirements, Tencent Cloud can provide dedicated personnel to assist and actively respond to audits or review activities initiated by the customer. Tencent Cloud also undergoes regular independent third-party professional audits and publishes assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status for service organizations.
10.2	Termination of Material Ongoing Outsourced Relevant Services	Upon the termination of the outsourcing agreement relating to a material ongoing outsourced relevant service, the bank in Singapore must ensure that all customer information given to the service provider or	When terminating material ongoing outsourced relevant services, customers should ensure that, where applicable, customer information provided to the service provider or subcontractor is promptly deleted, destroyed, or rendered unusable. Upon service termination, Tencent Cloud applies strict data erasure procedures. After the retention

No.	Domain	Summary of Controls	Tencent Cloud's Response
		sub-contractor, where applicable, are removed from the possession of the service provider or sub-contractor, as the case may be, or deleted, destroyed or rendered unusable as soon as possible except where – (a) the service provider or sub-contractor, as the case may be, is prohibited from doing so by written law or foreign laws, in the case where the material ongoing outsourced relevant service is performed overseas; or (b) in the case where the service provider or sub-contractor is a branch or office of the bank, the customer information is stored in a system used by the bank which upon the termination of the outsourcing agreement, can only be accessed by the bank.	period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable. If any media used to provide Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud will promptly perform complete physical destruction in accordance with rigorous internal processes. In terms of subcontractor management, Tencent Cloud has established a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers. This ensures that subcontracting does not impair its ability to provide relevant services to customers, the confidentiality and integrity of customer information processing, or the supervisory and audit rights of the Monetary Authority of Singapore and financial institutions.
10.3	Termination of Material Ongoing Outsourced Relevant Services	A bank in Singapore should consider whether to terminate the outsourcing agreement or cease receiving services under the following circumstances, and document the decision-making process: (a) the service provider or sub-contractor has failed to safeguard the confidentiality or integrity of information of the bank that is in the custody of the service provider or sub-contractor; (b) the service provider has failed to comply with any written law related to the provision of the material ongoing outsourced relevant service; (c) the service	Customers should, where appropriate, consider whether to terminate the outsourcing agreement or cease receiving services and document the decision-making process. Tencent Cloud delivers cloud services based on the Service Level Agreements (SLAs) defined for each service. Performance indicators, measurement standards, and reporting requirements are clearly specified in the SLA for each product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of cloud services and provides real-time monitoring through the management console. The written agreement between Tencent Cloud and the customer includes compliance and regulatory requirements, confidentiality and security information, business continuity and disaster

No.	Domain	Summary of Controls	Tencent Cloud's Response
		provider has undergone or is undergoing a change in ownership and where such a change might adversely affect whether the bank is able to satisfy itself of the service provider's ability to provide the material ongoing outsourced relevant service based on the framework in paragraph 5.1 of this Notice; (d) there has been a deterioration in the ability of the service provider to provide the material ongoing outsourced relevant service in accordance with the outsourcing agreement; (e) there has been a demonstrable deterioration in the ability of the service provider or sub-contractor, where applicable, to safeguard the confidentiality or integrity of the customer information in its custody; (f) the bank or any person appointed by the bank is prevented by the service provider, from obtaining any record, document, report or information relating to the provision of material ongoing outsourced relevant service; and (g) the bank is prevented by the service provider from assessing the service provider's compliance with the outsourcing agreement.	recovery, incident notification, contract termination clauses, data privacy and security, ownership and access rights, etc. If a customer needs to terminate the contract due to business changes or future IT planning, they may choose to back up and migrate cloud data and production environments at any time. Tencent Cloud supports customers in using standard formats for data backup or migration, enabling them to adopt the same transmission methods and protocols used during cloud onboarding, or utilize network services such as **Direct Connect (DC)** and **VPN Connection** to ensure secure and reliable data transfer during termination of cloud service engagement.

5.2 Requirements for Outsourcing Relevant Services Involving Customer Information

No.	Domain	Summary of Controls	Tencent Cloud's Response
12.2	Evaluation of Service Provider relating to Outsourced Relevant Services	12.2 For the purposes of the Act, before obtaining an outsourced relevant service which involves the disclosure of customer information, to evaluate the ability of the service provider to safeguard the confidentiality and integrity of customer information disclosed to, or accessed, collected, copied, modified, used, stored or processed by, the service provider, a bank in Singapore must conduct due diligence checks to assess and be satisfied of all of the following matters at the minimum: (a) the service provider's reputation and track record for safeguarding the confidentiality and integrity of customer information in its custody; (b) the service provider's ability to ensure that employees who are authorized to access the customer information are subject to confidentiality obligations; (c) the measures that the service provider has put in place to safeguard the confidentiality and integrity of customer information of the bank that is in the custody of the service provider, in relation to the provision of the relevant service.	Before obtaining outsourced services that involve the disclosure of their customer information, the customer should conduct due diligence on the service provider. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. Below is an overview of Tencent Cloud's capabilities in various aspects of due diligence as a cloud service provider: • **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. • **Confidentiality Obligation:**Tencent Cloud strictly adheres to laws and regulations governing user privacy and data security in all jurisdictions where it operates. It provides online legal documents such as Terms of Service, Data Processing and Security Agreement, which clearly define the protection of Customer data, intellectual property, and confidentiality obligations. Tencent Cloud requires internal employees to sign confidentiality undertakings that clearly define confidentiality obligations, while external personnel are bound by confidentiality clauses stipulated in agreements between Tencent Cloud and outsourcing vendors. • **Protection of Information Confidentiality and Integrity:**Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data content. Adhering to the principle of "data privacy," Tencent Cloud employs multi-layered technical isolation measures—such as virtualization control layer access policies, internal private network isolation strategies, web console permission allocation and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			identity authentication, session IDs and access keys—to ensure data segregation and prevent tenants from accessing, obtaining, or tampering with other tenants' data. Tencent Cloud's storage and database products support data encryption using strong, secure algorithms, integrated with the Key Management Service (KMS) for full lifecycle key management, ensuring data confidentiality.
12.3	Evaluation of Service Provider relating to Outsourced Relevant Services	A bank in Singapore must satisfy itself, on an ongoing basis, of the service provider's ability to safeguard the confidentiality and integrity of customer information disclosed to, or accessed, collected, copied, modified, used, stored or processed by, the service provider.	Customers should continuously assess the service provider's ability to protect the confidentiality and integrity of customer information under its custody. To support customers in meeting regulatory requirements, Tencent Cloud specifies audit and oversight rights for customers in the service agreement based on actual circumstances and provides dedicated personnel to assist and actively respond to investigations or review activities initiated by the customer. In addition, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes annual independent professional audits by domestic and international third parties and publishes assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, company shareholders, and other relevant stakeholders, providing transparency on Tencent Cloud's latest internal control status for service organizations. **For data storage protection,** 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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. Tencent Cloud also employs multi-replica redundant storage and erasure coding technology to ensure data integrity and initiate immediate recovery measures upon detecting errors, significantly improving fault tolerance. **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. • **Cloud Connect Network (CCN)**: 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,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			making data transmission secure and dependable.
12.8	Outsourcing Agreement and Access to Information relating to Outsourced Relevant Services	For the purposes of the Act, before obtaining an outsourced relevant service which involves the disclosure of customer information, a bank in Singapore must enter into an outsourcing agreement with the service provider, which must include all of the following: (a) a requirement that the service provider protects the confidentiality and integrity of all customer information; (b) a requirement that the service provider ensures that the service provider and its employees only access, collect, store, process or use any customer information to the extent that is necessary for the service provider to provide the outsourced relevant service; (c) a requirement that the service provider ensures that the service provider and its employees do not disclose any customer information to any third party unless compelled by law, in which case the service provider must notify the bank as soon as practicable to the extent permitted by law; (d) a requirement that the service provider, on a request by the bank, satisfies the bank, its auditors, the Authority or any	Before obtaining outsourced services that involve the disclosure of customer information, customers must enter into an outsourcing agreement with the service provider. The agreement should include clauses related to information confidentiality and integrity, restrictions on access to customer information, restrictions on disclosure of customer information, audit rights of banks and relevant regulators, rights to obtain service-related information, and service termination. 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, 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 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). If disclosure of customer data is legally mandated, Tencent Cloud will comply with relevant Singapore laws and promptly notify the customer. Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and

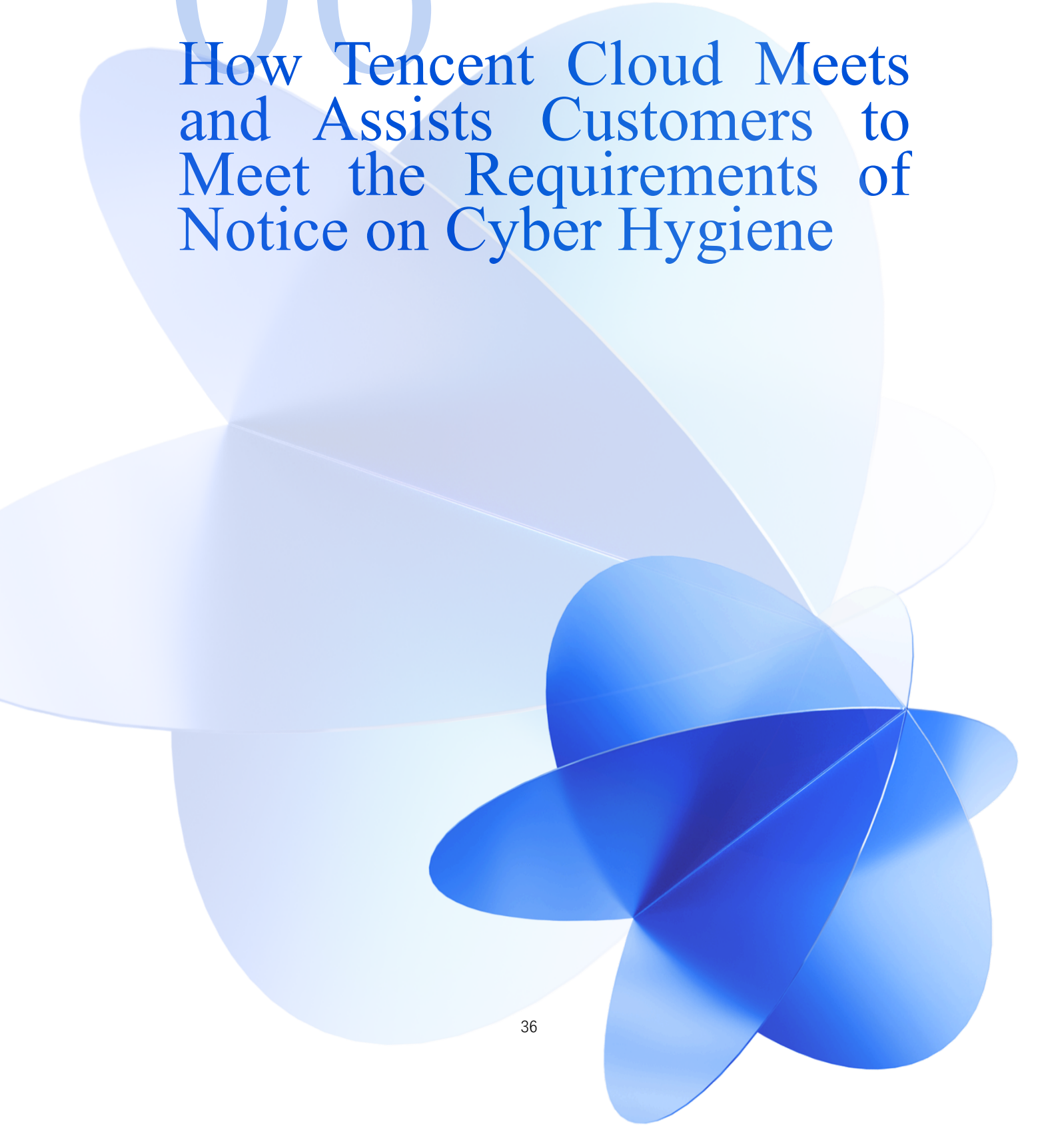
No.	Domain	Summary of Controls	Tencent Cloud's Response
		person appointed by the Authority, by the production of such evidence or information as the relevant person may require, that the service provider is in compliance with paragraph (a); (e) a requirement that the bank may terminate the outsourcing agreement or stop receiving the outsourced relevant service from the service provider under any of the following circumstances: (i) the service provider has failed to safeguard the confidentiality or integrity of the customer information in its custody; (ii) there has been a demonstrable deterioration in the ability of the service provider to safeguard the confidentiality or integrity of the customer information in its custody.	the reliability of business services, and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities. To ensure employees fulfill confidentiality obligations, Tencent Cloud requires internal staff to sign confidentiality agreements specifying their obligations and responsibilities, as well as potential penalties for violations. Outsourced personnel must also undergo background checks prior to employment and comply with confidentiality requirements stipulated in agreements between Tencent Cloud and subcontractors. Confidentiality requirements for employees and third parties are reviewed and updated by Tencent Cloud's legal department as needed. Upon customer request, Tencent Cloud will actively cooperate by providing information and, where necessary, furnish MAS or its designated personnel with records, documents, reports, or information related to the confidentiality and integrity of customer information. For more details on information access protection and confidentiality, please refer to Section 5.1 of this guide under clause "7.1 Outsourcing Agreements and Information Access Related to Material Ongoing Outsourced Relevant Services.
12.9	Protection of Customer Information relating to Outsourced Relevant Services	A bank in Singapore that receives an outsourced relevant service which involves the disclosure of customer information must implement adequate measures to protect such customer information that is disclosed to the service provider against unauthorized disclosure, access, collection, copying, use, modification, disposal or similar risks. The bank must at the minimum ensure that the measures include all of the following: (a) notifying the service	Customers should take measures to protect customer information disclosed to the service provider, preventing unauthorized disclosure, access, collection, copying, modification, use, disposal, or similar risks. This includes providing written notice to the service provider regarding both parties' legal obligations to maintain confidentiality of customer information and ensuring that the service provider and its employees access or use customer information only to the extent necessary for delivering outsourced services. Tencent Cloud strictly complies with privacy and data protection laws and regulations in the jurisdictions where it operates. Tencent Cloud offers online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		provider in writing of – (i) the bank's obligation to keep customer information confidential under the Act and common law; (ii) the service provider's obligation to keep customer information confidential under the Act; and (iii) in the case where the outsourced relevant service is to be performed outside Singapore, the bank's obligations to protect customer information in accordance with the laws of the place where the outsourced relevant service is to be performed; (b) ensuring that customer information is disclosed to, or accessed, collected, copied, modified, used, stored or processed by, a service provider and its employees only to the extent that is necessary for the service provider and its employees to provide the outsourced relevant service.	Data Processing and Security Agreement, which clearly define the scope and level of services provided, protection of user data and intellectual property, security responsibilities. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents). Tencent Cloud has established authorization policies and mechanisms. Permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights. For more details on customer information protection, please refer to Section 5.1 of this guide under clause "**8.1 Customer Information Protection Related to Material Ongoing Outsourced Relevant Services**."
12.11	Termination of Outsourced Relevant Services	Upon the termination of the outsourcing agreement relating to an outsourced relevant service that involves the disclosure of customer information or when a bank in Singapore stops obtaining or receiving an outsourced relevant service that involves the disclosure of customer information, the bank must ensure that all customer information given to the service provider are removed from the possession of the service	When terminating outsourced services that involve the disclosure of customer information, customers should, where applicable, promptly ensure that customer information provided to the service provider is deleted, destroyed, or rendered unusable. If customers need to temporarily discontinue use of the public cloud platform due to business changes or future IT planning, they may choose to back up and migrate cloud data and production environments at any time. Tencent Cloud supports customers in using standard formats for data backup or migration. **For data deletion and destruction**, Tencent Cloud provides secure and reliable data erasure mechanisms. Upon service termination, Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
		provider or deleted, destroyed or rendered unusable as soon as possible except where – (a) the service provider is prohibited from doing so by written law or foreign laws, in the case where the outsourced relevant service is performed overseas; or (b) in the case where the service provider is a branch or office of the bank in Singapore, the customer information is stored in a system used by the bank which upon the termination of the outsourcing agreement, can only be accessed by the bank.	Cloud applies strict data erasure procedures. After the retention period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Notice on Cyber Hygiene



Given the increasingly severe cyber threat landscape and to further strengthen the overall cyber resilience of financial institutions, the Monetary Authority of Singapore (MAS) has issued **Notice on Cyber Hygiene** for different types of financial institutions, including banks in Singapore, designated financial holding companies, licensed financial advisers, capital markets intermediaries, credit card or charge card licensees, merchant banks, insurers and insurance agents, registered insurance brokers, designated payment system licensees, operators and settlement institutions, finance companies, licensed trust companies, and licensed credit bureaus. These Notices set out a series of fundamental cybersecurity measures that financial institutions must implement to effectively address cyber threats.

The Notice prescribe cybersecurity requirements such as protecting administrative accounts, applying security patches, establishing baseline security standards, deploying network security devices, implementing anti-malware measures, and strengthening user authentication.

In this section, Tencent Cloud summarizes the control requirements in the Notice on Cyber Hygiene that are relevant to cloud service providers and explains how Tencent Cloud, as a CSP, assists financial institutions in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.1	Administrative Accounts	A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorized access to or use of such account.	Customers should protect and monitor administrator accounts to prevent unauthorized access or use. Customers can use **Cloud Access Management (CAM)** to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through **CloudAudit**. In addition, Tencent Cloud provides **Bastion Host (BH)**, which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. To support customers in meeting regulatory requirements, Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation

No.	Domain	Summary of Controls	Tencent Cloud's Response
			logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
4.2	Security Patches	(a) A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability. (b) Where no security patch is available to address vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system.	Customers should establish a vulnerability management mechanism to promptly apply security patches and remediate system vulnerabilities. For vulnerabilities that cannot be fixed through patches, compensating controls should be implemented. Customers can use **Cloud Workload Protection Platform (CWPP)** to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, receive real-time alerts, and obtain remediation plans to quickly address vulnerability risks. **Tencent Cloud Container Security Service (TCSS)** provides a virtual patching system designed to protect against frequently occurring zero-day vulnerabilities. It integrates Tencent's vulnerability discovery and real-time high-risk vulnerability alerting technologies to capture and analyse vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically apply them to cloud servers to effectively block hacking attempts. In addition, customers can use **Vulnerability Scanning Service (VSS)** to perform regular security scans on enterprise network devices and application services, receive continuous risk alerts and vulnerability detection, and obtain professional remediation recommendations to reduce security risks. To support customers in meeting regulatory requirements, Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform. Tencent Cloud uses a vulnerability scanning system to perform regular scans for security vulnerabilities across the cloud environment. The scanning scope covers the virtualization layer, system layer, and application layer. Upon completion of the scanning, the Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security team will analyze, categorize, and address the discovered vulnerabilities. Any identified security vulnerabilities are logged into the ticketing system to ensure they are properly handled within the stipulated timeframe. Tencent Cloud uses host endpoint detection tools to regularly scan patch installation status and records overdue patch installations in the ticketing system.
4.3	Security Standards	(a) A relevant entity must ensure that there is a written set of security standards for every system. (b) Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards. (c) Where the system is unable to conform to the set of security standards, the relevant entity must ensure that controls are instituted to reduce any risk posed by such non-conformity.	Customers should establish security standards for their systems, implement secure configurations, and perform baseline checks. For situations where baseline security configurations cannot be met, compensating controls should be implemented. Customers can use **Cloud Workload Protection Platform (CWPP)**, which leverages Tencent's extensive threat intelligence to help manage baseline security. CWPP supports baseline detection through options such as one-click checks and scheduled scans, and provides visibility into baseline compliance rates along with remediation recommendations. CWPP also offers Tencent Cloud's default baseline policies to help customers better manage server security baselines. **Cloud Security Center (CSC)** provides automated configuration risk assessments for cloud products, covering cloud servers, object storage, cloud databases, and load balancers, helping customers reduce risks caused by misconfigurations and improve overall cloud security posture. Customers can use **Configuration Audit (Config)** for centralized auditing and governance of cloud resources, continuously recording configuration details and changes across regions under the customer's account. Based on Tencent Cloud best-practice rules and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and

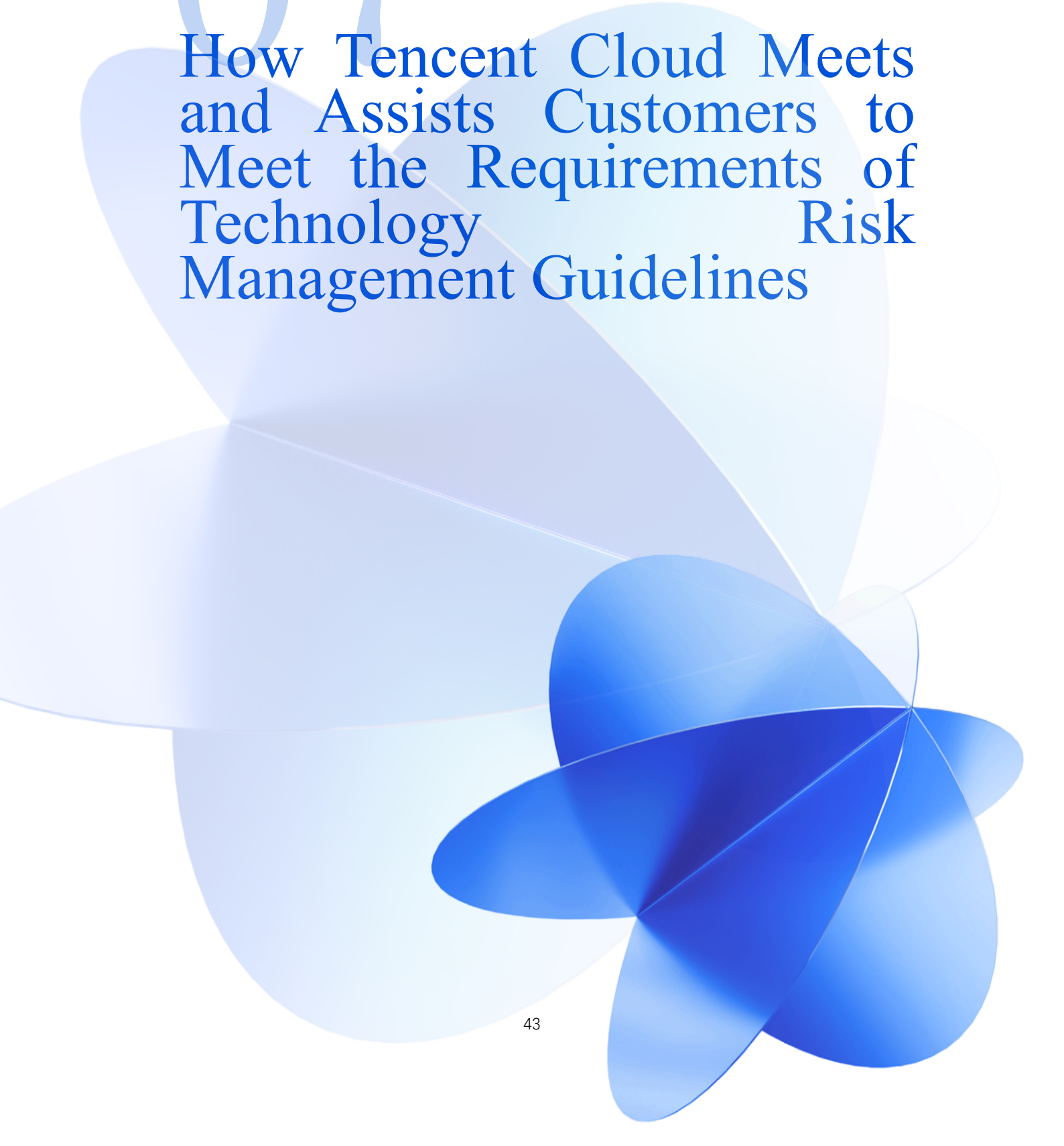
No.	Domain	Summary of Controls	Tencent Cloud's Response
			management of cloud resources. To support customers in meeting regulatory requirements, Tencent Cloud has also established internal network security configuration standards and baseline security standards to standardize configurations for network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud uses scanning tools to check configurations of operating systems, database management systems, network devices, and virtual images, continuously detecting and correcting deviations from baseline-defined standard configurations.
4.4	Network Perimeter Defense	A relevant entity must implement controls at its network perimeter to restrict all unauthorized network traffic.	Customers should implement necessary security controls at their network boundaries to restrict unauthorized network traffic. Tencent Cloud provides a range of security products to help customers achieve robust perimeter protection. For example, **Web Application Firewall (WAF)** helps both Tencent Cloud and external users defend against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and bot scraping. **Cloud Firewall (CFW)** offers protection across different network boundaries, addressing unified access control management and log auditing needs. It supports proactive firewall ACL control, IPS real-time interception, virtual patching, and malicious code detection; integrates Tencent's threat intelligence for real-time interception of abnormal outbound connections; and enables DMZ-like protection for core assets with fine-grained isolation between VPCs. Customers can also use **Anti-DDoS** services to mitigate DDoS attack risks. This service combines abundant, high-quality DDoS mitigation resources with evolving proprietary and AI-driven detection algorithms to ensure stable and secure business operations. Anti-DDoS offers multiple solutions, including basic protection for cloud servers and load balancers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			with real-time traffic monitoring and attack mitigation, as well as advanced high-availability services such as DDoS High Defence IP to prevent large-scale attacks that could disrupt services and cause financial losses. Additionally, Tencent Cloud provides an **EdgeOne (EO) platform**, leveraging global edge nodes to deliver security and acceleration services, including DDoS protection, intelligent web defence, bot/crawler attack prevention, DNS resolution, and customizable access control rules. To assist customers in meeting regulatory requirements, Tencent Cloud designs its network security architecture based on industry best practices, dividing security zones according to business functions and risk levels, and applying physical or logical isolation. Measures such as access control and perimeter defence ensure the security of office, and production networks. Tencent Cloud employs multiple layers of protection—including firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS mitigation, and web security defences—to counter various internet threats.
4.5	Malware protection	A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented.	Customers should implement or deploy anti-malware protection measures for their systems to mitigate the risk of malware infection. Customers can use **Cloud Workload Protection Platform (CWPP)** to secure cloud servers. CWPP leverages Tencent's extensive threat intelligence and machine learning to provide intrusion detection, vulnerability risk alerts, and other security services, including password cracking prevention, abnormal login alerts, Trojan file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by servers. To support customers in meeting regulatory requirements, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools for physical host security, enabling

No.	Domain	Summary of Controls	Tencent Cloud's Response
			comprehensive monitoring and control of all server endpoints across the network. The EDR solution provides antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing for command operations and login activities. It also triggers alerts upon detecting malicious programs or abnormal behaviors.
4.6	Multi-factor Authentication	A relevant entity must ensure that multi-factor authentication is implemented for the following: (a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and (b) all accounts on any system used by the relevant entity to access customer information through the internet.	Customers should implement multi-factor authentication (MFA) for administrator accounts on critical systems and for accounts that access confidential information over the Internet. Tencent Cloud provides **Cloud Access Management (CAM)** to help customers securely and granularly manage access to Tencent Cloud products and resources. CAM supports multiple methods of secondary identity verification, including MFA device validation or SMS verification codes, to ensure identity and environment security before login and sensitive operations. To support customers in meeting regulatory requirements, Tencent Cloud has also established internal access control policies and a privilege separation matrix. Tencent Cloud enforces Zero Trust security management for employee access, requiring two-factor authentication before accessing internal resources. In addition, Tencent Cloud's production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before accessing bastion hosts, and only authorized personnel can log in after completing secondary identity verification.

07

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Technology Risk Management Guidelines



In 2021, the Monetary Authority of Singapore (MAS) revised its Technology Risk Management Guidelines. These guidelines establish principles and best practices for managing technology risk in the financial sector, guiding financial institutions to build sound and robust technology risk governance and oversight mechanisms while maintaining cyber resilience. The requirements cover multiple areas, including overall technology risk governance and oversight, technology risk management frameworks, project management and secure design, software application development and management, IT service management, IT resilience, access control, cryptography, data and infrastructure security, cybersecurity operations, cybersecurity assessments, and IT audits.

In this section, Tencent Cloud summarizes the control requirements in the Technology Risk Management Guidelines that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in meeting these requirements.

7.1 Technology Risk Governance and Oversight

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.2	Policies, Standards and Procedures	3.2.1 The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets3 in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape. 3.2.2 The FI should ensure risks associated with deviations are thoroughly reviewed and assessed. The risk assessment should be approved by senior management. Approved deviations should be reviewed periodically to ensure the residual risks remain at an acceptable level. 3.2.3 Compliance processes should be implemented to verify that policies, standards	Customers should establish and maintain policies, standards, and procedures for technology risk management and the protection of information assets, and review and update them regularly. This ensures that any deviations from established policies, standards, or procedures are thoroughly examined and assessed, and identified risks are addressed promptly. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and procedures are adhered to. These include follow-up processes for non-compliance.	team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. For any identified deviations, the team analyzes actual or potential causes, evaluates the need and priority for corrective and preventive actions, and implements these measures upon obtaining the necessary approvals. A dedicated oversight group tracks and records the effectiveness of corrective actions.
3.3	Management of Information Assets	3.3.1 The FI should establish information asset management practices that include the following: (a)identification of information assets that support the FI′ s business and delivery of financial services; (b)classification of an information asset based on its security classification or criticality; (c)ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and (d)establishment of policies, standards and procedures to manage information assets according to their security classification or criticality. 3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes.	Customers should maintain an inventory of all information assets and establish an information asset management mechanism to identify, classify, and assign ownership of assets. Security controls should be applied based on the classification level of each asset. The asset inventory should be reviewed regularly and updated promptly whenever changes occur. To assist customers in comprehensive information asset management, Tencent Cloud provides **Cloud Workload Protection Platform (CWPP),** which supports automated collection of asset fingerprints and unified management of asset fingerprint data such as accounts, ports, processes, and applications. CWPP can also conduct rapid investigations into the risk impact scope of security incidents that have occurred based on asset fingerprints, helping customers enhance server security. Customers can also adopt Tencent Cloud's one-stop security management platform, **Cloud Security Center (CSC)**, for information asset security management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such as cloud configuration risks, vulnerabilities, and security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			events, thereby reducing the risk of "shadow IT" on the cloud. To support customers in complying with control principles, Tencent Cloud has formulated information asset management specifications and full-lifecycle management processes, which conduct classified and hierarchical management and protection of assets such as electronic data, hardware and their virtual devices, infrastructure, application systems, and software. Tencent Cloud manages hardware devices and software components through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, etc. This ensures the stable operation of the underlying system of the cloud platform and provides reliable support for business systems.
3.4	Management of Third Party Services	3.4.3 On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality4 and integrity as well as ensuring system resilience.	Customers should conduct due diligence on third-party organizations regarding data confidentiality, integrity, and system resilience. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon customer requirements, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. Specifically for Singapore, Tencent Cloud has achieved DPTM (Data Protection Trustmark) certification, MTCS Tier 3 (Multi-Tier Cloud Security) certification, Cyber Trust Mark and complies with the Association of Banks in Singapore (ABS) Outsourcing Guidelines, demonstrating that Tencent Cloud's security and privacy protection capabilities meet relevant certification standards and industry best

No.	Domain	Summary of Controls	Tencent Cloud's Response
			practices. Tencent Cloud undergoes professional third-party audits annually. For more details on due diligence, please refer to Section 8: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions (Non-Bank Financial Institutions)," **Clause 3.3.2/5.4.2 "Evaluation of Service Providers."**
3.5	Competency and Background Review	3.5.1 The FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks. 3.5.2 Insider threat, which includes theft of confidential data, sabotage of IT systems and fraud by staff, contractors and service providers, is considered one of the risks to an organization. A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimize this risk.	Customers should ensure that all employees, contractors, and service providers possess the necessary competence and skills to perform IT functions and manage technology risks. Background checks should be conducted on individuals who have access to financial institution data and IT systems. To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive Human Resources Security Management Standard, which specifies the review process during recruitment. This includes verifying academic qualifications, professional certifications, integrity records, and any criminal history. In addition, Tencent Cloud's Human Resources department is responsible for conducting background checks on new hires and updating them as needed.
3.6	Security Awareness and Training	3.6.1 A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI. All personnel in the FI should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets. 3.6.2 The training programme should be conducted at least annually for all staff,	Customers should establish an information security awareness training program and conduct security awareness training at least annually for all personnel authorized to access information assets. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Framework, which requires all formal employees, consultants, interns, and outsourced staff to complete information security training courses. These courses include mandatory training for all staff, specialized training for key roles, and optional professional courses. The training content covers areas such as basic security awareness,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		contractors and service providers who have access to the FI′ s information assets.	office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.

7.2 Technology Risk Management Framework

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.1	Risk Management Framework	4.1.1 The FI should establish a risk management framework to manage technology risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities, and clear reporting lines across the various organizational functions. 4.1.2 Effective risk management practices and internal controls should be instituted to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment. 4.1.3 The risk owner, who is accountable for ensuring proper risk treatment measures are implemented and enforced for a specific technology risk, should be identified. 4.1.4 The framework should also cover risk identification, risk assessment, risk treatment and risk monitoring, review and reporting. 4.1.5 The FI should review the adequacy and effectiveness of its risk management framework	Customers should establish a risk management framework and implement effective risk management practices and controls. Customers should regularly review their risk management framework, identify and assess risks, assign risk owners, develop and implement risk mitigation measures for identified risks, and continuously monitor risks. To support customers in meeting regulatory requirements, Tencent Cloud has defined an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessments regularly, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. Furthermore, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		regularly.	
4.2	Risk Identification	4.2.1 The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers.	Customers should regularly identify threats and vulnerabilities applicable to their IT environment, analyze and assess the risks posed by these threats and vulnerabilities, prioritize risks, develop risk mitigation measures, evaluate residual risks, and monitor the effectiveness of risk control measures. To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. • **Risk Identification:** Tencent Cloud conducts risk assessments regularly, identifying applicable risk scenarios from sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. • **Risk Assessment:** Tencent Cloud evaluates asset value, the likelihood of risk scenarios, and the potential impact, then calculates the risk level. • **Risk Treatment:** Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items, the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• **Risk Monitoring, Review, and Reporting:** Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions.

7.3 IT Project Management and Security-by-Design

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.3	System Acquisition	5.3.1 The FI should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverable to the FI. 5.3.2 It is important that the FI assesses the robustness of the vendor ' s software development and quality assurance practices, and ensures stringent security practices are in place to safeguard and protect any sensitive data the vendor has access to over the course of the project. Any vendor access to the FI′ s IT systems should be	Customers should establish standards and procedures for vendor evaluation and selection and perform an appropriate level of assessment and due diligence based on the criticality of project deliverables. In addition, customers should assess vendors' software development and quality assurance processes and implement monitoring measures to safeguard sensitive data within their IT systems. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon customer requirements, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. Specifically for Singapore, Tencent Cloud has achieved DPTM (Data Protection Trustmark) certification, MTCS Tier 3 (Multi-Tier Cloud Security) certification,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		controlled and monitored.	Cyber Trust Mark and complies with the Association of Banks in Singapore (ABS) Outsourcing Guidelines, demonstrating that Tencent Cloud's security and privacy protection capabilities meet relevant certification standards and industry best practices. Tencent Cloud undergoes professional third-party audits annually. For more details on due diligence, please refer to Section 8: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions (Non-Bank Financial Institutions)," **Clause 3.3.2/5.4.2 "Evaluation of Service Providers."** Tencent Cloud integrates the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System into the entire secure product development lifecycle. This approach covers all stages—requirements, design, development, testing, delivery, and operations—embedding information security and privacy protection principles throughout the product lifecycle to ensure robust security controls and assessments. Customer data is classified as a high-security-level data within Tencent Cloud. Full control over customer data remains with the customer; Tencent Cloud does not attempt to access or disclose customer content. Tencent Cloud provides a comprehensive operations security mechanism, requiring all production environment operations to be performed through bastion hosts. Access to bastion hosts requires prior authorization and only authorized internal operations personnel can log in after completing secondary identity verification. This ensures that the operations service team cannot directly access customer information assets without

No.	Domain	Summary of Controls	Tencent Cloud's Response
			explicit customer consent and authorization.
5.4	System Development Life Cycle and Security-By-Design	5.4.1 The FI should establish a framework to manage its system development life cycle (SDLC). Standards and procedures for the different phases of the SDLC should be maintained. 5.4.2. The FI should incorporate security specifications in the system design, perform continuous security evaluation, and adhere to security practices throughout the SDLC. 5.4.3 Security requirements should minimally cover key control areas such as access control, authentication, authorization, data integrity and confidentiality, system activity logging, security event tracking and exception handling. 5.4.4 The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.	Customers should establish a system development lifecycle (SDLC) management framework and incorporate security requirements into every stage of the SDLC. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information System Secure Development Standard and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the secure product development lifecycle. This approach covers all phases—requirements, design, development, testing, delivery, and operations. At each stage, Tencent Cloud involves security teams to validate security requirements, ensuring that cloud products receive adequate security controls and assessments throughout their lifecycle, thereby reducing information security and privacy risks. Security requirements include, but are not limited to, identity and access management, data security, network security, and security auditing.
5.5	System Requirements Analysis	5.5.1 The FI should identify, define and document the functional requirements for the IT system. In addition to functional requirements, it should also establish and document key non-functional requirements. 5.5.2 In establishing the	Customers should identify, define, and document the functional requirements of IT systems, and ensure that security requirements meet the acceptable security level necessary for their business needs. To support customers in meeting regulatory requirements, Tencent Cloud incorporates both functional and non-functional requirements during each product iteration, drawing from

No.	Domain	Summary of Controls	Tencent Cloud's Response
		security requirements, the FI should assess the potential threats and risks related to the IT system and determine the acceptable level of security required to meet its business needs.	sources such as user feedback, project stakeholders, product brainstorming sessions, and operational activities. During the requirements analysis phase, Tencent Cloud conducts security requirement analysis and business risk assessment. The project manager invites relevant teams—such as testing and security teams—to perform a security review of the product requirements specification. This process involves discussions on business content, workflows, and technical architecture to identify the optimal approach for embedding security.
5.6	System Design and Implementation	5.6.1 The FI should review the proposed architecture and design of the IT system, to ensure they meet the defined requirements, before implementation. 5.6.2 The FI should verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be endorsed by relevant stakeholders. 5.6.3 Relevant domain experts should be engaged to participate in the design review.	Customers should review proposed IT system architecture and design prior to implementation and verify that the current system design meets the defined system requirements. To support customers in meeting regulatory requirements, Tencent Cloud analyses formally reviewed product requirements and, based on their complexity, determines whether a detailed technical plan is needed. Such a plan should include overall design, detailed design, implementation approach, testing strategy, resource allocation, and risk management. The project manager invites relevant teams—such as testing and security teams—to conduct security analysis and technical risk assessment of the product design. This process includes threat modelling for system design and security technical evaluations of the chosen architecture to ensure that functionalities are not implemented using insecure methods.
5.7	System Testing and Acceptance	5.7.1 A methodology for system testing should be established. A test plan should be established and approved before testing. 5.7.2 The FI should ensure each requirement is covered by appropriate test cases.	Customers should establish a system testing mechanism and develop and approve a test plan before testing begins. When changes occur in existing IT systems, regression testing should be performed. All issues identified during testing should be addressed promptly, and a test report should be prepared for stakeholder confirmation. In addition, customers should maintain a separate physical or logical environment for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		5.7.3 The FI should maintain separate physical or logical environments for unit, system integration and user acceptance testing, and restrict access to each environment on a need-to basis. 5.7.4 The FI should perform regression testing for changes to an existing IT system to validate that it continues to function properly after the changes have been implemented. 5.7.5 Issues identified from testing, including system defects or software bugs, should be properly tracked and addressed. Major issues that could have an adverse impact on the FI′ s operations or delivery of service to customers should be reported to the project steering committee and addressed prior to deployment to the production environment. 5.7.6 The FI should ensure the results of all testing that was conducted are documented in the test report, and signed off by the relevant stakeholders.	testing. To support customers in meeting regulatory requirements, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams. Tencent Cloud's change and release management process covers changes to applications, configuration files, operating systems, and databases. All changes must undergo independent functional testing before deployment. After implementing changes, Tencent Cloud's business team performs critical path regression validation to ensure changes meet expectations and do not introduce abnormal behaviour or performance degradation, thereby maintaining overall system stability and availability. Furthermore, 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.
5.8	Quality Management	5.8.1 During project planning, the FI should define the expected quality attributes and the assessment metrics for the project deliverables based on its quality control standards.	Customers should perform quality assurance on project activities and deliverables in accordance with their quality control standards. To support customers in meeting regulatory requirements, Tencent Cloud is among the first cloud service providers in China to obtain

No.	Domain	Summary of Controls	Tencent Cloud's Response
		5.8.2 Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI′ s policies, procedures and standards.	ISO/IEC 9001 Quality Management System (QMS) certification in the cloud computing domain, having initially passed certification by an independent international audit body in 2015. Tencent Cloud strictly adheres to the requirements of ISO/IEC 9001:2015 and its organizational context to establish a comprehensive QMS. This includes a Quality Management Manual, quality policies and objectives, and related standards and procedural documents. The QMS provides a structured framework and systematic guidance for product quality management and daily operations, covering the entire lifecycle of Tencent Cloud products and services—planning, design and development, quality control, quality assurance, after-sales service, and continuous improvement—ensuring effective implementation of quality management practices. To maintain the applicability and effectiveness of the QMS, Tencent Cloud has implemented a quality audit program, which includes regular performance measurement, internal and external audits, and management reviews to ensure compliance with quality policies and objectives. Additionally, Tencent Cloud undergoes annual surveillance audits by independent third-party certification bodies to verify the compliance and effectiveness of its ISO/IEC 9001 QMS.

7.4 System Development Life Cycle and Security-By-Design

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.1	Secure Coding, Source Code Review and Application Security Testing	6.1.1 The FI should adopt standards on secure coding, source code review and application security testing. 6.1.2 The secure coding and source code review standards should cover areas such as	Customers should adopt secure coding standards, source code reviews, and application security testing measures to prevent software vulnerabilities or defects. Tencent Cloud's **Cloud Native Build (CNB)** provides a complete developer toolchain, including code hosting, high-performance CI/CD

No.	Domain	Summary of Controls	Tencent Cloud's Response
		secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling. 6.1.3 A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI′ s software. 6.1.4 The FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI′ s software. 6.1.5 The FI should ensure its software developers are trained or have the necessary knowledge and skills to apply the secure coding and application security standards when developing applications. 6.1.6 It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The software validation and testing rules should be reviewed periodically and kept current. 6.1.7 All issues and software defects discovered from the source code review and application security testing should be tracked. Major issues and software defects should be	pipelines, AI code assistant, and artifact management. The AI code assistant, designed specifically for developers, supports multiple mainstream programming languages and offers features such as code completion, unit testing, code diagnostics, intelligent reviews, and smart Q&A for code issues—helping developers improve coding quality and efficiency. **For secure coding and code review**, Tencent Cloud has established detailed secure coding guidelines that internal developers must strictly follow. Tencent Cloud provides secure programming training to enhance developers' awareness of risks such as injection attacks and sensitive data leaks. During development, developers are required to consider security features within application systems to minimize vulnerabilities. Tencent Cloud's internal code security analysis framework integrates capabilities such as Static Application Security Testing (SAST), open-source component scanning, and sensitive information detection. Business teams can leverage pipeline-based self-service scanning during the code admission phase to perform security assessments. Typical issues identified during code reviews are documented and consolidated into the team's knowledge base. Code review standards cover detection of vulnerabilities such as XSS, SQL injection, code execution, command injection, historical vulnerabilities in third-party components, and sensitive information protection. **For application security scanning**, Tencent Cloud requires business teams to connect web application test environments to web vulnerability scanning tools for automated scanning before product launch. If vulnerabilities are detected, tickets are automatically generated and assigned to the responsible development team for remediation prior to release, ensuring security issues are not carried into production. **For third-party product usage**, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		remediated before production deployment.	has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies.
6.2	Agile Software Development	6.2.1 When adopting Agile software development methods, the FI should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process. 6.2.2 The FI should ensure secure coding, source code review and application security testing standards are applied during Agile software development.	Customers should incorporate Software Development Lifecycle (SDLC) principles and security-by-design practices into agile development processes. Customers can leverage **Cloud Native Build (CNB)**, which is deeply integrated with agile development concepts. From issues and merge requests to task sets, CNB provides a structured agile workflow, enabling customers to validate product iterations quickly and cost-effectively before market release. **Tencent Infrastructure Automation for Terraform** offers automated deployment, implementation, and management of Tencent Cloud resources through Terraform—a globally recognized Infrastructure-as-Code (IaC) tool—facilitating DevOps practices and multi-cloud deployments. Tencent Cloud embeds essential SDLC principles and Security-by-Design concepts throughout its agile development process. The secure product development lifecycle incorporates information security and privacy protection across all stages—requirements analysis, design, development, testing, delivery, and operations—ensuring robust security controls throughout the product lifecycle. Key security measures include: • Security Training: Promoting secure coding awareness among developers and enforcing strict adherence to secure coding standards. • Requirements Analysis: Security integration is considered during business

No.	Domain	Summary of Controls	Tencent Cloud's Response
			process and technical framework discussions. • System Design: Threat modeling and security assessments are performed on system architecture. • System Development: Tencent provides secure development components for use during coding, following Tencent Cloud's secure coding guidelines. • Security Validation: Vulnerabilities are identified through code security checks, asset scans, web scans, manual security assessments, penetration testing, and code audits. • Release: Only after all high-risk issues have been fixed can the system be released to production to prevent vulnerabilities from being introduced into live environments. For more details on secure coding, source code review, and application security testing, refer to Section 7.4 "System Development Life Cycle and Security-By-Design," **Clause 6.1 "Secure Coding, Source Code Review, and Application Security Testing."**
6.3	DevSecOps Management	6.3.1 The FI should ensure its DevSecOps activities and processes are aligned with its SDLC framework and IT service management processes. 6.3.2 The FI should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.	Customers should adopt a DevSecOps management framework and apply the principle of segregation of duties for software development, testing, and release functions within this process. Customers can leverage **Cloud Native Build (CNB)**, which provides a complete developer toolchain to streamline the end-to-end development lifecycle—from requirements to deployment—enabling seamless integration of requirements, code, artifacts, and CI/CD. CNB facilitates efficient cross-functional collaboration, ensuring stable and continuous software delivery. Additionally, CNB integrates automated security capabilities such as source code sensitive information scanning and artifact scanning, creating an automated security detection pipeline

No.	Domain	Summary of Controls	Tencent Cloud's Response
			from coding and building to testing and deployment, delivering both quality and efficiency. To support customers in meeting regulatory requirements, Tencent Cloud incorporates its Software Development Lifecycle (SDLC) into the DevSecOps process to ensure rapid and continuous development, release, and deployment of cloud products. Tencent Cloud has also established access control authorization policies and a privilege separation matrix to enforce segregation of duties among personnel responsible for development, testing, and release activities.
6.4	Application Programming Interface Development	6.4.5 Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.	Customers should adopt encryption standards and key management controls to ensure the security of sensitive data transmitted via APIs. As the cornerstone of Tencent Cloud's open ecosystem, **TencentCloud API** Is cover services provided externally through this interface and are continuously enhanced. Tencent Cloud's Cloud APIs support HTTPS transmission encryption and implement multiple SDK-based signature mechanisms (such as PHP, Python, Java, .NET, Node.js) for API authentication. Additionally, Tencent Cloud uses Timestamp-based signature expiration to prevent replay attacks. Signature encryption supports HmacSHA1 and the more secure HmacSHA256, ensuring the integrity and security of API requests and providing port-level communication security for customers' business operations.
		6.4.7 Detective measures should be instituted to provide visibility of the usage and performance of APIs, and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.	Customers should establish detection mechanisms to visualize API usage and performance, promptly identify suspicious activities, and implement necessary measures to defend against cybersecurity attacks. Tencent Cloud offers multiple products to help customers monitor API usage and performance, such as:

No.	Domain	Summary of Controls	Tencent Cloud's Response
		6.4.8 The FI should ensure adequate system capacity is in place to handle high volumes of API call requests, and implement measures to mitigate cyber threats such as denial of service (DoS) attacks.	• **Web Application Firewall (WAF):** Provides a one-stop solution for web business risk protection. Its API security capabilities enable enterprises to inventory and manage API assets, intelligently detect dynamic changes and risk trends, accurately identify API exposure, sensitive data, and risk events, and apply protection rules with one click to mitigate API-related risks. • **TencentCloud API** monitoring features, allowing customers to configure API status monitoring via the console. Tencent Cloud also provides API protection capabilities to prevent API failures or misuse effectively. • **CloudAudit:** Automatically records and stores event logs of operations performed via Tencent Cloud APIs or the console by accounts and sub-accounts within the past seven days, simplifying compliance audits. • **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.

7.5 IT Service Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.2	Configuration Management	7.2.1 The FI should implement a configuration management process to maintain accurate information of its hardware and software to have visibility and effective control of its IT systems. 7.2.2 The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure it is accurate and up to	Customers should implement configuration management for the hardware and software required by their IT systems and regularly review and verify the accuracy and timeliness of configuration information. Customers can use **Cloud Security Center (CSC)** to automate dynamic inventory of cloud assets, including cloud servers, object storage, cloud databases, and load balancers. CSC also provides unified management of asset security risks across multiple dimensions, such as configuration risks, vulnerabilities, and security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		date.	events, helping reduce the risk of "shadow IT" in the cloud. To support customers in meeting regulatory requirements, Tencent Cloud has established a Configuration Management Policy and uses a Configuration Management Database (CMDB) to centrally manage IT service components and configuration items (CIs), including their relationships. When configuration updates occur during change processes, operations personnel update the version and related information of configuration items in the CMDB according to the change plan. Tencent Cloud conducts regular asset inventories and audits the CMDB to ensure the validity, accuracy, and completeness of configuration information.
7.3	Technology Refresh Management	7.3.1 The FI should avoid using outdated and unsupported hardware or software, The FI should closely monitor the hardware's or software's end-of-support (EOS) dates. 7.3.2 A technology refresh plan for the replacement of hardware and software should be developed before they reach EOS. A risk assessment for hardware and software approaching EOS date should be conducted to evaluate the risks of their continued use, and effective risk mitigation measures should be implemented. 7.3.3 The FI should obtain dispensation from its management for the continued use of outdated and unsupported hardware and software. The dispensation should be assigned a validity	Customers should establish a technology refresh plan, conduct risk assessments for hardware and software approaching end-of-support, and replace them upon expiration. If expired hardware or software continues to be used, management approval must be obtained. To support customers in meeting regulatory requirements, Tencent Cloud maintains a detailed inventory of hardware and facilities in its Configuration Management Database (CMDB), including each server's End-of-Support (EOS) date and version information. Tencent Cloud regularly retires and replaces servers, while software components (such as operating systems and database systems) are upgraded to appropriate versions before reaching end-of-support. For decommissioned hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction in official logs.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		period that is commensurate with the identified risks and risk mitigation measures. The dispensation should be reviewed periodically to ensure the attendant risks remain at an acceptable level.	
7.4	Patch Management	7.4.1 A patch management process should be established to ensure applicable functional and non-functional patches are implemented within a timeframe that is commensurate with the criticality of the patches and the FI′ s IT systems. 7.4.2 Patches should be tested before they are applied to the FI ′ s IT systems in the production environment to ensure compatibility with existing IT systems or they do not introduce problems to the IT environment.	Customers should establish a patch management process to apply patches based on their severity and the criticality of IT systems and conduct testing before implementation. Customers can use **Cloud Workload Protection Platform (CWPP)** to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, receive real-time alerts, and obtain remediation plans to quickly address vulnerability risks. **Tencent Cloud Container Security Service (TCSS)** provides a virtual patching system designed to protect against frequently occurring zero-day vulnerabilities. It integrates Tencent's vulnerability discovery and real-time high-risk vulnerability alerting technologies to capture and analyse vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically apply them to cloud servers to effectively block hacking attempts. In addition, customers can use **Vulnerability Scanning Service (VSS)** to perform regular security scans on enterprise network devices and application services, receive continuous risk alerts and vulnerability detection, and obtain professional remediation recommendations to reduce security risks. To support customers in meeting regulatory requirements, Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform. Tencent Cloud uses a vulnerability scanning system to perform regular scans for security vulnerabilities across the cloud environment. The scanning scope covers the virtualization layer,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. Tencent Cloud uses host endpoint detection tools to regularly scan patch installation status and records overdue patch installations in the ticketing system.
7.5	Change Management	7.5.1 The FI should establish a change management process to ensure changes to information assets are assessed, tested, reviewed and approved before implementation. 7.5.2 A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover factors such as security and implications of the change in relation to other information assets. 7.5.3 The FI should ensure all changes are adequately tested in the test environment. Test plans for changes should be developed and approved by the relevant business and IT management. Test results should be accepted and signed off before the changes are deployed to the production environment. 7.5.4 A change advisory board, comprising key stakeholders, should be formed to approve	Customers should establish a change management procedure to ensure that any changes to information assets are assessed, tested, reviewed, and approved prior to implementation. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also maintains an emergency change management process, under which emergency changes must receive appropriate approval before execution. All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment. Tencent Cloud classifies change requests based on attributes such as importance, urgency, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and prioritize the changes. 7.5.5 The FI should perform a backup of the information asset prior to the change implementation, and establish a rollback plan. 7.5.6 The FI should clearly define the procedures for assessing, approving and implementing emergency changes, as well as identify the authorizers or approvers for the changes. 7.5.7 The FI should ensure the logging facility is enabled to record activities that are performed during the change process.	scope of impact. For changes that may affect external environments—such as product, infrastructure, or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels.
7.6	Software Release Management	7.6.1 Segregation of duties in the software release process should be practiced to ensure no single individual has the ability to develop, compile and move software codes from one environment to another. 7.6.2 It is important that controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.	Customers should implement segregation of duties in the software release process and apply necessary controls to ensure the traceability and integrity of software code across all IT environments. To support customers in meeting regulatory requirements, Tencent Cloud has established release and deployment management standards. These standards include creating release plans to organize the software release process in a controlled manner, deploying release packages to target environments under managed conditions, reducing risks during release and deployment, minimizing impact on production operations, and ensuring business continuity. Additionally, Tencent Cloud performs integrity checks on software packages after they are uploaded to the production environment and applies version control to maintain software package integrity and traceability. Tencent Cloud has also implemented an access control authorization policy and a role-separation

No.	Domain	Summary of Controls	Tencent Cloud's Response
			matrix to ensure segregation of duties among personnel involved in software development, testing, and release. Furthermore, Tencent Cloud enforces strict internal network isolation rules, using both physical and logical isolation to ensure that development, and production environments remain segregated.
7.7	Incident Management	7.7.1 The FI should establish an incident management framework with the objective of restoring an affected IT service or system to a secure and stable state, as quickly as possible, so as to minimize impact to the FI′ s business and customers. 7.7.2 The FI should ensure sufficient resources are available to facilitate and support incident response and recovery. 7.7.3The incident management framework should minimally cover: (a)the process and procedure for handling IT incidents; (b)maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and (c)the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents. 7.7.4 The FI should configure system events or alerts to provide an early indication of issues that may affect its IT	Customers should establish incident management procedures and processes and configure system events and alert mechanisms to enable proactive monitoring and timely alerts. In the event of a major incident, customers should promptly report the incident status to senior management. In addition, customers should develop a communication plan that defines the relevant parties to contact and the content to be communicated when an incident occurs. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—**Cloud Security Center (CSC)**. Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the efficiency of security operations. **For internal incident management**, Tencent Cloud has established incident and service request management procedures and formulated an incident management policy. This ensures that all incidents related to IT service management activities are recorded and categorized, prioritized based on impact and urgency, and escalated as needed to ensure rapid resolution and closure. These measures minimize the impact of incidents, maintain normal business operations, and enhance customer satisfaction. **Regarding incident communication and notification**, Tencent Cloud has developed an

No.	Domain	Summary of Controls	Tencent Cloud's Response
		systems' performance and security. System events or alerts should be actively monitored so that prompt measures can be taken to address the issues early. 7.7.5 The FI should regularly apprise its senior management of the status of major incidents so that decisions to mitigate the impact of the crisis can be made in a timely manner. 7.7.6 A communications plan that covers the process and procedures to apprise customers of impact on services, and to handle media or public queries should be maintained. The plan should also include identifying the spokespersons and subject matter experts to address the media or public queries as well as the communication channels to disseminate information. 7.7.7 It would be useful for the FI to provide timely updates to its customers on the progress of its incident management and the measures the FI is implementing to protect its customers and continue delivery of financial services. Where appropriate, the FI should advise its customers on actions that they should take to protect themselves.	information security incident management standard, which includes procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. **For customer-initiated reporting or inquiries**, Tencent Cloud offers a ticketing service via the Tencent Cloud console, allowing customers to report faults, incidents, problems, and complaints related to security, availability, and confidentiality. In addition, Tencent Cloud provides online customer service and telephone support through the console and official website, enabling customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates multi-region redundant customer service centers that provide 24/7 support, ensuring continuous handling of customer requests, round-the-clock technical assistance for cloud products, and timely, high-quality service responses. Customers may also choose applicable service plans to access dedicated support groups, a designated technical account manager, and value-added services as part of a tailored support offering.
7.8	Problem Management	7.8.1 The FI should establish problem management process and procedures to determine and resolve the root cause of	Customers should establish problem management processes and procedures, maintain records of past incidents, analyse root causes, identify commonalities, and capture lessons learned to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		incidents to prevent the recurrence of similar incidents. 7.8.2 The FI should maintain a record of past incidents which include lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics. 7.8.3 A trend analysis of past incidents should be performed by the FI to identify commonalities and patterns in the incidents and verify if the root causes to the problems had been properly identified and resolved. The FI should also use the analysis to determine if further corrective or preventive measures are necessary.	prevent similar incidents from recurring. Tencent Cloud has implemented problem management standards that leverage event data and trend analysis to identify root causes and develop solutions, minimizing the impact of incidents and problems on business operations. Tencent Cloud centrally manages knowledge related to problem resolution to improve handling efficiency and adopts preventive measures to avoid repeated incidents, thereby enhancing service quality. Tencent Cloud uses an internal security operations system to record and track security incidents. After remediation and resolution, the responsible departments assess the cause, type, impact, and accountability of each incident and produce an information security incident investigation report. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type, frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review.

7.6 IT Resilience

No.	Domain	Summary of Controls	Tencent Cloud's Response
8.1	System Availability	8.1.1 IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs. 8.1.2 Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system	Customers should ensure that IT system design and implementation achieve an availability level that meets business requirements. For IT systems requiring high availability, redundancy solutions should be deployed and tested regularly to ensure resilience aligns with business needs. To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, organized by regions and availability zones, covering

No.	Domain	Summary of Controls	Tencent Cloud's Response
		availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.	Mainland China, Asia-Pacific, North America, and Europe. In Singapore, Tencent Cloud has deployed four leased data centers. Customers can flexibly deploy data and systems across different regions or availability zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures. Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point device failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability. Additionally, Tencent Cloud develops disaster recovery drill plans based on its Business Continuity Plan (BCP), conducts risk assessments for drills, and implements safeguards to prevent negative service impacts. Disaster recovery drills often simulate real-world scenarios, including attack-defence exercises and large-scale failures, to comprehensively validate system resilience, response speed, and recovery capability.
		8.1.3 The FI should continuously monitor the utilization of its system resources against a set of pre-defined thresholds. Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs.	Customers should continuously monitor system resource utilization, set performance and capacity thresholds, and implement necessary processes to manage situations where predefined thresholds are exceeded. To support customers in efficient capacity planning and adjustment, Tencent Cloud provides **Auto Scaling (AS)** services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		8.1.4 Procedures should be established to respond to situations when pre-defined thresholds for system resources and system performance have been breached.	policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. To enable effective monitoring and management of system performance, customers can use **Tencent Cloud Observability Platform (TCOP)**. This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services.
8.2	System Recoverability	8.2.1 The FI should establish systems' recovery time objectives (RTO) and recovery point objectives (RPO) that are	Customers should define RTO and RPO for their business systems, establish disaster recovery plans, review and update them regularly, and conduct periodic testing of these plans. In

No.	Domain	Summary of Controls	Tencent Cloud's Response
		aligned to its business resumption and system recovery priorities. 8.2.2 The FI's disaster recovery plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of relevant personnel in the recovery process. The disaster recovery plan should be reviewed at least annually and updated when there are material changes to business operations, information assets or environmental factors. 8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management. The FI should avoid deviating from the plan as untested recovery measures could exacerbate the incident and prolong the recovery process. In exceptional circumstances where untested recovery measures need to be used, the FI should perform a risk assessment and ensure adequate controls are in place, as well as obtain approval from senior management. 8.2.4 The FI should endeavor to operate from its recovery, secondary or alternate site periodically so as to have the assurance that its infrastructure and systems at these sites are able to support business needs	addition, customers should periodically operate business processes at recovery sites, backup sites, or alternate sites to ensure these locations can support continuous operations in the event of a failure. Tencent Cloud offers a wide range of products designed with high availability features to help customers achieve system and service resilience. For example: • **Cloud Load Balancer (CLB)** 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. • **Cloud Virtual Machine (CVM)** 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. • **Cloud Object Storage (COS)** provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • **TencentDB for MySQL** supports high reliability and availability with robust automatic backup and lossless recovery mechanisms. • **Tencent Kubernetes Engine (TKE)** 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		for an extended period of time when production systems fail over from the primary or production site.	services and data. Tencent Cloud ensures complete isolation between different regions, maximizing stability and fault tolerance. Each region is further divided into multiple isolated availability zones to reduce the impact of single-point failures and guarantee business continuity for customers. To ensure business continuity for customers, Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud computing environment and has obtained international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud conducts Business Impact Analysis (BIA) for its cloud products and services to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Based on BIA results, Tencent Cloud develops appropriate strategies and business continuity plans, including detailed disaster recovery plans for cloud products. Tencent Cloud regularly performs business continuity drills and tests to validate the feasibility of these plans and procedures. For more details on business continuity, please refer to Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management."
8.3	Testing of Disaster Recovery Plan	8.3.1 The FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the defined recovery objectives. Relevant stakeholders should participate in the disaster recovery test to familiarize themselves with the recovery processes and ascertain if the systems are	Customers should regularly test their disaster recovery (DR) plans to validate their effectiveness. For information assets managed by service providers, customers should assess the provider's disaster recovery capabilities and collaborate with the provider to conduct joint testing. Customers can leverage the **Cloud Advisor (TSA)** service to assist with planning and executing business continuity tests. This service is a cloud governance platform that integrates multiple ITOM vertical applications and draws

No.	Domain	Summary of Controls	Tencent Cloud's Response
		performing as expected. 8.3.2 A disaster recovery test plan should include the test objectives and scope, test scenarios, test scripts with details, system recovery procedures, and the criteria for measuring the success of the test. 8.3.3 The testing of disaster recovery plan should comprise: (a)various plausible disruption scenarios; and (b)recovery dependencies between information assets. 8.3.4 Where information assets are managed by service providers, the FI should assess the service provider's disaster recovery capability and ensure disaster recovery arrangements for these information assets are established, tested and verified to meet its business needs. The FI should engage its service provider to test the recovery steps that require coordinated actions between the service provider and the FI.	on Tencent Cloud's extensive operational expertise. Through risk inspections, fault drills, and other governance measures, Cloud Advisor optimizes cloud infrastructure. It provides fault injection scenarios across IaaS and PaaS layers, as well as industry-specific drill templates covering typical use cases such as cross-availability zone disaster recovery. This helps customers quickly and efficiently reuse proven solutions based on their business needs, improving system availability. To ensure continuous availability of customer services, Tencent Cloud develops tailored response strategies and business continuity plans based on business impact analysis of its products and services. Detailed disaster recovery plans are established for cloud products and critical processes, covering facilities, personnel, equipment, systems, information/data, and business priorities. Tencent Cloud designs drill plans based on its business continuity framework, conducts risk assessments for drills, and implements safeguards to prevent negative impacts on services. Disaster recovery drills typically simulate real-world scenarios, including attack-defense exercises and large-scale failures, to comprehensively test system resilience, response speed, and recovery capability. After each drill, relevant departments prepare a drill report, implement corrective actions, and archive the report for recordkeeping. If the customer assesses that the disaster recovery drill requires Tencent Cloud's participation and collaboration, Tencent Cloud will respond promptly and fully cooperate. Based on the specific needs of the customer, Tencent Cloud will clearly define the scenario and scope of the drill, jointly formulate a detailed drill plan and execution schedule. During the drill, Tencent Cloud will provide necessary technical support and resource guarantees, assist the customer in continuously optimizing the disaster recovery

No.	Domain	Summary of Controls	Tencent Cloud's Response
			strategy and process, and jointly enhance business continuity and disaster recovery capabilities.
8.4	System Backup and Recovery	8.4.1 The FI should establish a system and data backup strategy, and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted. 8.4.2 The FI should institute a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data. 8.4.3 The FI should periodically test the restoration of its system and data backups to validate the effectiveness of its backup restoration procedures. 8.4.4 To protect data in backup from unauthorized access and modification, the FI should ensure any confidential data stored in the backup media is secured. Backup media should be stored offline or at an offsite location.	Customers should establish a backup management mechanism to back up confidential and sensitive data, encrypt backup storage media, apply physical protection, and conduct regular backup recovery tests. Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customer needs, such as: • Cloud Object Storage (COS): 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. • Cloud Block Storage (CBS): 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. • Cloud File Storage (CFS): Offers scheduled snapshot capabilities for flexible backup task configuration. • Cloud Native Database TDSQL-C: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • TencentDB for MySQL: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • TencentDB for MongoDB: Offers automated backup and lossless recovery mechanisms, supporting multi-node

No.	Domain	Summary of Controls	Tencent Cloud's Response
			backups and retention of multiple days of backup data for disaster recovery scenarios.
8.5	Data Centre Resilience	8.5.1 The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centers (DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.	Customers should conduct threat and vulnerability risk assessments for their data centers and establish appropriate protective measures. As a cloud service provider, Tencent Cloud is committed to delivering secure, stable, continuous, and reliable physical infrastructure for customers. Currently, Tencent Cloud operates four leased data centers in the Singapore region. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts annual on-site audits to verify that data center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures.
		8.5.2 The FI should ensure adequate redundancy for the power, network connectivity, and cooling, electrical and mechanical systems of the DC to eliminate any single point of failure. 8.5.3 As part of the DC's	Customers should ensure that data centers have sufficient redundancy in power supply, network connectivity, cooling systems, and electromechanical systems to eliminate any single points of failure. To support customers in meeting regulatory requirements, Tencent Cloud ensures that all global data centers are selected, constructed, or

No.	Domain	Summary of Controls	Tencent Cloud's Response
		environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems.	leased in compliance with relevant international standards and local security requirements. For leased data centers in the Singapore region, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity, Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the data center.
		8.5.4 The FI's secondary or disaster recovery DC should be geographically separated from its primary or production DC so that both sites will not be impacted by a disruption to the underlying infrastructure (e.g. telecommunications and power) in a particular location.	Customers should ensure that their backup or disaster recovery data centers are geographically separated from their primary data centers. Tencent Cloud's infrastructure is deployed across multiple global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an isolated fault domain with physical separation. Customers can flexibly deploy data and systems across different regions or availability zones based on business growth needs and data security requirements to meet disaster recovery objectives.
		8.5.5 The DC's physical security and environmental controls should be monitored on a 24 by 7 basis. Appropriate escalation, response plans and procedures for physical and environmental incidents at DCs should be established and tested. 8.5.6 The DC should have adequate physical access	Customers should implement necessary monitoring and access control measures for data centers to ensure physical and environmental security. **For physical access control**, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		controls including: (a)access granted to staff should be on a need-to-have basis, and revoked promptly if access is no longer required; (b)proper notification and approval for visitors to the DC. All visitors should be escorted by authorized staff at all times while in the DC; (c)physical access points in the DC should be secured and monitored at all times; access to equipment racks should be restricted to authorized staff and monitored; (d)access to keys and other physical access devices should be restricted to authorized staff, and replaced or changed promptly if they have been misplaced, lost or stolen; and (f)segregation of delivery and common areas from security sensitive areas should be enforced.	promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). **For security and monitoring**, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. **For physical and environmental incidents**, Tencent Cloud requires operators to establish escalation mechanisms, response plans, and handling procedures, and to conduct regular drills to validate these processes. This ensures rapid response and resolution of such incidents, minimizing their impact on Tencent Cloud's platform and services.

7.7 Access Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.1	User Access Management	9.1.1 The principles of 'never alone', 'segregation of duties', and 'least privilege' should be applied when	Customers should implement appropriate identity authentication and access control mechanisms to manage access to information assets and establish effective password policies.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		granting staff access to information assets so that no one person has access to perform sensitive system functions. 18 Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers. 9.1.2 The FI should establish a user access management process19 to provision, change and revoke access rights to information assets. Access rights should be authorized and approved by appropriate parties. 9.1.4 The FI should establish a password policy and a process to enforce strong password controls20 for users' access to IT systems. 9.1.5 Multi-factor authentication21 should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorized access. 9.1.6 The FI should ensure appropriate parties perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user	Cloud Access Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions. Through the CAM console, customers can configure password policies for sub-users, including complexity, length, and validity period. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to customer passwords, ensuring that plaintext passwords are never stored. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. To support regulatory compliance, Tencent Cloud has also established internal access control authorization policies and a role-separation matrix. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud enforces zero-trust security management for employee access, requiring login and completion of multi-factor authentication before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions only when necessary and through a rigorous approval process. Tencent Cloud maintains records mapping job roles to identity information and system permission levels and conducts regular internal permission reviews to prevent misuse or abuse of access rights.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		access review should be resolved as soon as practicable. 9.1.7 Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status, should be revoked or disabled promptly.	
		9.1.3 For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes. 9.1.8 The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.	Customers should log all user access records and user management activities to facilitate auditing and investigations. Customers can use **Cloud Access Management (CAM)** to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through **CloudAudit**. In addition, Tencent Cloud provides **Bastion Host (BH)**, which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. If customers encounter any issues related to accounts, network security, or product usage, they can submit a support ticket through the console to obtain technical assistance. Tencent Cloud provides a comprehensive operational security framework to ensure that service teams cannot directly access customer information assets without explicit customer consent and authorization.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			To support regulatory compliance, Tencent Cloud implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to 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.
9.2	Privileged Access Management	9.2.1 Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring. 9.2.2 The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorized activities.	Customers should implement controls over privileged accounts, including secure storage, approval processes, usage logging, and monitoring. Cloud Access Management (CAM) provides granular permission control, allowing customers to assign specific permissions to different personnel for different resources. In addition, customers can use CloudAudit to monitor Tencent Cloud account activities, perform compliance checks, operational reviews, and risk audits. CloudAudit supports online viewing of Tencent Cloud console and cloud API operation records for up to 90 days. Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
9.3	Remote Access Management	9.3.1 Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorized access to the FI's IT environment. 9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards.	Customers should grant remote access permissions only as necessary and implement appropriate security controls for such access. Customers can also use **VPN Connection** to establish secure communication between their on-premises data centers and Tencent Cloud resources. The VPN tunnel uses Internet Key Exchange (IKE) and IPsec protocols to encrypt transmitted data, creating a secure and trusted data tunnel over the Internet. The VPN gateway is highly reliable, built on a master/slave hot backup architecture, ensuring uninterrupted communication sessions and seamless failover that is imperceptible to upper-layer applications. To enable customers to securely and quickly access cloud business systems anytime, anywhere, and from any mainstream device, Tencent Cloud supports SSL VPN technology for remote access. SSL VPN encrypts data transmitted over the Internet to ensure security and provides access control mechanisms to reduce unauthorized access. Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect through encrypted communication channels to access Tencent Cloud's corporate network and office systems remotely. Tencent Cloud maintains remote access logs to record user activities. Furthermore, Tencent Cloud's internal office network is completely isolated from the production environment where Customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data

No.	Domain	Summary of Controls	Tencent Cloud's Response
			resides through a bastion host with two-factor authentication. When granting permissions, Tencent Cloud enforces fine-grained access controls to ensure employees receive only the minimum privileges necessary to deliver the required service. Requests for additional permissions must undergo multi-level review and approval. All backend maintenance operations are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these records.

7.8 Cryptography

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.1	Cryptographic Algorithm and Protocol	10.1.2 The FI should adopt cryptographic algorithms from well-established international standards. The FI should also select an appropriate algorithm and encryption key length that meet its security objectives and requirements. 10.1.3 Where the security of the cryptographic algorithm depends on the unpredictability of a random seed or number, the FI should ensure the seed or random number is of sufficient length and randomness. 10.1.4 The FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements. 10.1.5 The FI should monitor developments in the area of cryptanalysis and, where necessary, update or change the	Customers should adopt internationally recognized cryptographic algorithms, ensuring that all algorithms undergo rigorous testing and evaluation to meet security objectives and requirements. To protect the confidentiality and integrity of Customer data, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength cryptographic algorithms. These products integrate with the **Key Management Service (KMS)** to provide full lifecycle management of encryption keys, ensuring data confidentiality. To support regulatory compliance, Tencent Cloud has established encryption and key management standards that mandate the use of cryptographic algorithms during data transmission and storage. For key management, Tencent Cloud selects cryptographic products and algorithms that comply with international cryptographic policy requirements. Customer communications on the Tencent Cloud console are protected by the HTTPS security protocol. Tencent Cloud's cloud products provide API interfaces with HTTPS encryption, signature verification, and status

No.	Domain	Summary of Controls	Tencent Cloud's Response
		cryptographic algorithms or increase the key lengths to ensure they remain resilient against evolving threats.	monitoring capabilities, ensuring port-level communication security for customer business operations.
10.2	Key management	10.2.1 Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established. 10.2.2 The FI should ensure cryptographic keys are securely generated and protected from unauthorized disclosure. Any cryptographic key or sensitive data used to generate or derive the keys should be also be protected or securely destroyed after the key is generated. 10.2.3 The FI should determine the appropriate lifespan of each cryptographic key based on factors, such as the sensitivity of the data, the criticality of the system to be protected, and the threats and risks that the data or system may be exposed to. The cryptographic key should be securely replaced, before it expires at the end of its lifespan. 10.2.4 To protect sensitive cryptographic keys, the FI should manage, process and store such keys in hardened and tamper resistant systems, e.g. by using a hardware security module. 10.2.5 Where sensitive	Customers should establish cryptographic key management policies, standards, and procedures covering key generation, distribution, installation, rotation, revocation, recovery, and expiration. To help customers protect the confidentiality, integrity, and availability of keys, Tencent Cloud provides the **Key Management Service (KMS)**. KMS enables customers to easily create and manage keys, meeting multi-application and multi-business key management needs while complying with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, allowing customers to apply encryption effortlessly. KMS is built on FIPS 140-2 certified Hardware Security Modules (HSMs) for key generation and protection, uses secure data transmission protocols, and employs a multi-data-center distributed cluster architecture with hot backups. Underlying HSM devices are deployed with dual-site cold backups to ensure high availability of the key management system. To maintain ciphertext security and reduce the risk of key compromise or misuse, KMS supports regular key rotation. Rotated keys remain compatible with previously encrypted data, ensuring no impact on customer operations. KMS securely deletes expired, invalid, or compromised keys using irreversible methods, making deleted keys unrecoverable and rendering associated encrypted data permanently inaccessible. For financial institutions, where communication and stored data are highly sensitive and valuable, KMS provides envelope encryption for protocol

No.	Domain	Summary of Controls	Tencent Cloud's Response
		cryptographic keys need to be transmitted, the FI should ensure these keys are not exposed during transmission. The keys should be distributed to the intended recipient via an out-of-band channel or other secure means to minimize the risk of interception. 10.2.6 Cryptographic keys should be used for a single purpose. For instance, the cryptographic key for data encryption should be different from the one that is used to generate cryptographic digital signatures. 10.2.7 If a cryptographic key is found to be compromised, the FI should revoke and replace the key and all other keys whose security could also be compromised as a result of the exposed key. 10.2.8 When cryptographic keys have expired or have been revoked, the FI should use a secure key destruction method to ensure the keys are not recoverable. 10.2.9 When replacing or renewing a compromised or expiring cryptographic key, the FI should generate the new key in a manner such that any adversary who has knowledge of part or whole of the previous key will not be able to derive the new key from it. 10.2.10 The FI should maintain backups of cryptographic keys	communications, critical files, and documents, along with key protection and access control to meet security and compliance requirements. Key transmission and distribution processes are encrypted using TLS 1.2 to prevent man-in-the-middle attacks. 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		for recovery purposes and accord them a high level of protection.	

7.9 Data and Infrastructure Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
11.1	Data Security	11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorized access, modification, copying, or transmission of its confidential data, taking into consideration the following: Data in Motion、Data at Rest and Data in Use. 11.1.2 The FI should implement appropriate measures to prevent and detect data theft, as well as unauthorized modification in systems and endpoint devices. The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards. 11.1.3 Confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.	Customers should establish a comprehensive data loss prevention (DLP) policy and implement necessary measures such as data encryption and access controls to prevent and detect unauthorized access, modification, or theft of data. Tencent Cloud provides **Data Security Audit (DSA)**, an AI-powered database security auditing system. DSA supports comprehensive auditing of session information, access operations, and SQL statements across enterprise networks, leveraging multiple rule libraries and threat detection engines to identify malicious behaviors and promptly notify administrators to take appropriate security measures. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access Customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with applicable laws and regulations during investigations by national or local authorities. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities. Additionally, Tencent Cloud deploys DLP tools on employee computers to restrict external data export and monitor, detect, and prevent potential data exfiltration attempts. To ensure confidentiality and integrity of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customer data during storage, Tencent Cloud's storage and database products support encryption using secure, high-strength algorithms and integrate with the **Key Management Service (KMS)** for full lifecycle key management. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations.
		11.1.6 The use of sensitive production data in non-production environments should be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval has to be obtained from senior management. The FI should ensure appropriate controls are implemented in non-production environments to manage the access and removal of such data to prevent data leakage. Where possible, such data should be masked in the non-production environments.	Customers should restrict the use of sensitive production data in non-production environments; if absolutely necessary, senior-management approval must be obtained and the data must be de-identified. 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.
		11.1.7 The FI should ensure confidential data is irrevocably deleted from storage media, systems and endpoint devices before they are disposed of or redeployed.	Customers should restrict the use of sensitive production data in non-production environments. If such use is necessary, it must be approved by senior management and the data must be properly masked. Tencent Cloud enforces strict separation of development, testing, and production environments through physical and logical isolation and prohibits the use of unmasked production data in non-production environments. Customers should ensure that confidential data

No.	Domain	Summary of Controls	Tencent Cloud's Response
			stored on media, systems, and endpoint devices is irreversibly deleted before disposal or redeployment. Tencent Cloud provides secure and reliable data destruction mechanisms. When a customer's service is terminated, Tencent Cloud follows strict data erasure procedures to completely remove Customer data before reusing any previously purchased compute or storage resources. If media used to deliver Tencent Cloud services fails and requires replacement or reaches end-of-life, Tencent Cloud promptly performs thorough physical destruction in accordance with strict processes.
11.2	Network Security	11.2.1 The FI should install network security devices such as firewalls to secure the network between the FI and the Internet, as well as connections with third parties. 11.2.2 The FI should deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system ' s functional role (e.g. database and application) or the sensitivity of the data. 11.2.3 Network intrusion prevention systems should be deployed in the FI' s network to detect and block malicious network traffic. 11.2.4 The FI should implement network access controls to detect and prevent unauthorized devices from connecting to its network.	Customers should implement network segmentation based on system criticality or data sensitivity and deploy network security devices such as firewalls, intrusion prevention systems (IPS), and DDoS protection. In addition, customers should enforce network access control measures to prevent unauthorized devices from connecting to the network and regularly review access control rules. **For network segmentation or partitioning**, customers can use Tencent Cloud's **Virtual Private Cloud (VPC)** service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. To implement network perimeter protection, Tencent Cloud offers the **EdgeOne (EO) platform**, which provides security and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		11.2.5 Network access control rules in network devices should be reviewed on a regular basis to ensure they are kept up-to-date. Obsolete rules and insecure network protocols should be removed promptly. 11.2.6 The FI should consider isolating internet web browsing activities from its endpoint devices through the use of physical or logical controls, or implement equivalent controls, so as to reduce exposure of its IT systems to cyber attacks. 11.2.7 An effective DoS protection should be implemented to detect and respond to various types of DoS attacks. 22 The FI could engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI′ s network infrastructure. 11.2.8 A review of the FI′ s network architecture, including should be conducted on a periodic basis to identify potential cyber security vulnerabilities.	acceleration services through Tencent's global edge nodes. EO includes DDoS protection, intelligent web defense, bot/crawler attack mitigation, DNS resolution, and supports custom access control rules. Customers can also use Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services. **Cloud Firewall (CFW)** provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. **Web Application Firewall (WAF)** helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. **Anti-DDoS** combines abundant, high-quality DDoS mitigation resources with continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks, ensuring stable and secure business operations. **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, effectively preventing cross-tenant data access or tampering. Tencent Cloud has established **network security management standards and a defense-in-depth architecture**. Security domains are defined based on business functions and risk levels, with

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. For Internet browsing security, 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. Tencent Cloud regularly reviews its network security architecture and protection strategies, including firewall, IPS/IDS, and DDoS configurations, to identify vulnerabilities and update security rules. All network architecture and device changes follow a strict change management process, including impact analysis, rollback planning, and formal approval before implementation.
11.3	System Security	11.3.1 The security standards for the FI' s hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimize their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness. 11.3.2 The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely	Customers should establish security standards for their hardware and software, implement secure configurations, and set up processes to verify deviations between system configurations and security standards. Customers can use **Cloud Workload Protection Platform (CWPP)**, which leverages Tencent's extensive threat intelligence to help manage baseline security. CWPP supports baseline detection through options such as one-click checks and scheduled scans, and provides visibility into baseline compliance rates along with remediation recommendations. CWPP also offers Tencent Cloud's default baseline policies to help customers better manage server security baselines. **Cloud Security Center (CSC)** provides automated configuration risk assessment for cloud products, covering cloud servers, object storage, cloud databases, and load balancers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		manner.	helping customers reduce risks caused by misconfigurations and improve overall cloud security posture. Customers can use Configuration Audit (Config) for centralized auditing and governance of cloud resources, continuously recording configuration details and changes across regions under the customer's account. Based on Tencent Cloud best-practice rules and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. To support customers in meeting regulatory requirements, Tencent Cloud has established a set of network security configuration standards and security baseline standards aimed at standardizing the security configuration of network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud uses scanning tools to check the configurations of operating systems, database management systems, network devices, and virtual images, continuously detecting deviations from the standard configurations defined in baseline files. Once a deviation is identified, the system automatically generates a security ticket and sends it to the responsible department for timely remediation.
		11.3.3 Endpoint protection, which includes but is not limited to behavioral-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware. 11.3.4 The FI should ensure that anti-malware signatures are kept up-to-date and the systems are regularly scanned	Customers should implement endpoint protection measures, deploy antivirus software to perform regular system scans, and promptly update virus definitions to monitor and identify abnormal activities on endpoint systems. Customers can use Cloud Workload Protection Platform (CWPP) to secure cloud servers. CWPP leverages Tencent's extensive threat intelligence and machine learning to provide intrusion detection, vulnerability risk alerts, and other security services, including password cracking prevention, abnormal login alerts, Trojan

No.	Domain	Summary of Controls	Tencent Cloud's Response
		for malicious files or anomalous activities. 11.3.5 To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems′ , including endpoint systems′ , processes for anomalies and suspicious activities. 11.3.6 Security measures, should be implemented to ensure only authorized software is allowed to be installed on the FI′ s systems	file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by servers. **To support customers in meeting regulatory requirements**, 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 Terminal endpoint protection**, Tencent Cloud has established an internal software-security baseline that clearly defines which applications may be installed on corporate laptops and workstations, and enforces an application-whitelisting policy that allows only known, trusted programs to run, thereby reducing the risk of malware infection. A zero-trust endpoint-management platform provides additional controls, including antivirus scanning, vulnerability patching, and active-defense capabilities that deliver comprehensive protection against ransomware, phishing, and lateral-movement attacks.
11.4	Virtualization Security	11.4.1 The FI should ensure security standards are established for all components of a virtualization solution. 11.4.2 Strong access controls should be implemented to restrict administrative access to the hypervisor and host operating system. 11.4.3 The FI should establish policies and standards to manage virtual images and	Customers should establish policies to manage the creation, distribution, storage, usage, decommissioning, destruction, and security of virtual machine images and snapshots, and implement controls to restrict administrator-level access to hypervisors and host operating systems. Tencent Cloud provides **Cloud Virtual Machine (CVM)**, a scalable virtualization compute 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
		snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorized access or modification.	Tencent Cloud initialization components. CVM also supports custom image creation, image import, sharing, and deletion. Additionally, CVM provides snapshot functionality, including manual and scheduled snapshots, to support scenarios such as routine backups, rapid data recovery, and fast environment deployment. To ensure CVM security, customers can configure security groups and network ACLs to define host and network access policies, enabling flexible firewall settings for different instances. CVM supports sensitive operation protection, requiring identity verification before executing critical actions. Tencent Cloud also provides Cloud Monitor, offering real-time alerts and security services such as DDoS protection, DNS hijacking detection, intrusion detection, vulnerability scanning, web shell detection, and login protection. For container image management, **Tencent Cloud Container Registry (TCR)** offers secure, dedicated, 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, delivering full lifecycle protection from image creation and storage to runtime. **To strengthen security controls for virtual machines and virtualization services**, Tencent Cloud has established internal virtualization security management standards, defining responsibilities for resource management, access control, and configuration management. Tencent Cloud employs technologies such as virtual machine isolation, resource control, patch management, vulnerability protection, and hypervisor hardening to build a comprehensive

No.	Domain	Summary of Controls	Tencent Cloud's Response
			virtualization security defence system.

7.10 Cyber Security Operations

No.	Domain	Summary of Controls	Tencent Cloud's Response
12.1	Cyber Threat Intelligence and Information Sharing	12.1.1 To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyze cyber-related information for its relevance and potential impact to the FI′ s business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.	Customers should develop network security situational awareness capabilities to collect, process, and analyze cybersecurity-related information that may impact business and IT environments. To support customers in threat detection and analysis, Tencent Cloud provides the **Threat Intelligence Center (TIX)**, a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. TIX is SaaS-based and supports multiple delivery methods, including web portals, APIs, SDKs, TIP integration, and mini-programs, meeting varied customer needs. It can also integrate with customers' existing security products to enhance overall security operations and threat response efficiency. Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable.
12.2	Cyber Event Monitoring and Detection	12.2.1 The FI should establish a security operations center or acquire managed security services. The processes, roles and responsibilities for security operations should be defined. 12.2.2 A process to collect, process, review and retain system logs should be established to facilitate the FI′s security monitoring operations. These logs should be protected against unauthorized access. 12.2.3The FI should establish a baseline profile of each IT system′s routine activities and analyze the system activities against the baseline profiles. The profiles should be regularly reviewed and updated. 12.2.4 The FI should consider applying user behavioral analytics to enhance the effectiveness of security monitoring. User behavioral analytics might include the use of machine learning algorithms in real time to analyze system logs, establish a baseline of normal user activities and identify suspicious or anomalous behaviors. 12.2.5 Correlation of multiple events registered on system logs should be performed to identify	Customers should establish a Security Operations Center (SOC) or use managed security services to ensure timely detection and response to cybersecurity incidents. In addition, customers should implement a log management mechanism to collect, process, and analyze system logs to identify suspicious or abnormal activities. Customers may use **Cloud Log Service (CLS)**, a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. The **Cloud Security Center (CSC)** aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Customers can also use Cloud Audit to record logs and continuously monitor account activity across Tencent Cloud infrastructure. **Elasticsearch Service (ES)** enables customers to stream real-time logs from cloud servers, containers, and other cloud products, as well as ingest historical and incremental business data into Tencent Cloud ES clusters for distributed storage and analytical queries. Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Tencent Cloud also operates an internal network monitoring system to monitor and alert on

No.	Domain	Summary of Controls	Tencent Cloud's Response
		suspicious or anomalous system activity patterns. 12.2.6 A process should be established to ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behavior.	network devices such as routers, firewalls, and servers, and uses a ticketing system to track and resolve identified security issues. Tencent Cloud has defined detailed operational security "red lines" and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts.
12.3	Cyber Incident Response and Management	12.3.1 The FI should establish a cyber incident response and management plan to swiftly isolate and neutralize a cyber threat and to securely resume affected services. The plan should describe communication, coordination and response procedures to address plausible cyber threat scenarios. 12.3.2 As part of the plan, the FI should establish a process to investigate and identify the security or control deficiencies that resulted in security breach. The investigation should also evaluate the full extent of the impact to the FI. 12.3.3 Information from cyber intelligence and lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.	Customers should establish a network security incident management and response mechanism to quickly eliminate cybersecurity threats and perform root cause analysis of incidents, enabling lessons learned and continuous improvement of the incident response process. To support customers in incident detection and rapid response, Tencent Cloud provides the **Cloud Security Center (CSC)**, a one-stop security management platform. CSC offers features such as Asset Center, Risk Center, Alert Center, and advanced security management, helping customers achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving security operations efficiency. Internally, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. Tencent Cloud also maintains a periodic incident analysis mechanism, conducting multi-dimensional reviews (e.g., incident type, frequency, scope, and severity) and implementing preventive measures based on post-incident

No.	Domain	Summary of Controls	Tencent Cloud's Response
			reviews and root cause analysis to prevent recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review. Additionally, Tencent Cloud's security team operates a 24/7 security operations framework, focusing on vulnerability monitoring, intrusion tracing, and attack mitigation. The team responds to alerts in real time, quickly conducts attack forensics, and formulates emergency response plans to effectively contain incident spread. For more details on incident detection, response, and communication, please refer to Section 7.5 IT Service Management, clause "**7.7 Incident Management**."

7.11 Cyber Security Assessment

No.	Domain	Summary of Controls	Tencent Cloud's Response
13.1	Vulnerability Assessment	13.1.1 The FI should establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the IT system and the security risk to which it is exposed. 13.1.2 When performing VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, and open network ports, as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on	Customers should regularly conduct vulnerability assessments and penetration tests to identify security weaknesses and evaluate their cybersecurity defense capabilities. For penetration testing, Tencent Cloud offers the **Cloud Pressure Testing (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. For vulnerability scanning, customers can use the **Vulnerability Scanning Service (VSS)** to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive

No.	Domain	Summary of Controls	Tencent Cloud's Response
		common web-based vulnerabilities.	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.
13.2	Penetration Testing	13.2.1 The FI should carry out penetration testing (PT) to obtain an in-depth evaluation of its cyber security defenses. 13.2.2 The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT. 13.2.3 PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment. 13.2.4 The frequency of PT should be determined based on factors such as system criticality and the system's exposure to cyber risks. For systems that are directly accessible from the Internet, the FI is expected to conduct PT to validate the adequacy of the security controls at least once annually or whenever these systems undergo major changes or updates.	To support regulatory compliance, Tencent Cloud regularly schedules vulnerability scans for cloud environment assets and analyzes, categorizes, and remediates detected vulnerabilities. Tencent Cloud also conducts full-chain large-scale penetration tests to proactively identify and fix potential security risks and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated via security tickets to responsible departments for timely remediation or compensating controls. Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.
13.3	Cyber Exercises	13.3.1 The FI should carry out regular scenario-based cyber exercises to validate its response and recovery, as well as communication plans against cyber threats. 13.3.2 Depending on the exercise objectives, the FI should involve relevant	Customers should regularly conduct scenario-based cybersecurity emergency drills to validate response capabilities and communication effectiveness, and invite relevant stakeholders to participate. Tencent Cloud's internal business units periodically conduct scenario-based training and drills for security incident response plans. Tencent Cloud also provides ongoing technical training for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		stakeholders.	its security teams based on evolving technologies and threat landscapes, ensuring staff understand and comply with the latest security standards and best practices and can respond quickly and effectively to security incidents. If the customer assesses that the disaster recovery drill requires Tencent Cloud's participation and collaboration, Tencent Cloud will respond promptly and fully cooperate. Based on the specific needs of the customer, Tencent Cloud will clearly define the scenario and scope of the drill, jointly formulate a detailed drill plan and execution schedule. During the drill, Tencent Cloud will provide necessary technical support and resource guarantees, assist the customer in continuously optimizing the disaster recovery strategy and process, and jointly enhance business continuity and disaster recovery capabilities.
13.4	Adversarial Attack Simulation Exercise	13.4.1 The FI should perform an adversarial attack simulation exercise32 to test and validate the effectiveness of its cyber defense and response plan against prevalent cyber threats. 13.4.2 The objectives, scope and rules of engagement should be defined before the commencement of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team do not disrupt the FI′ s production systems.	Customers should regularly conduct adversarial attack simulation exercises and ensure that such exercises are performed in a controlled environment without impacting the production systems of financial institutions. Tencent Cloud regularly conducts red team vs. blue team exercises simulating real-world cyberattacks to test and validate its ability to respond to network attacks.
13.5	Intelligence-Based Scenario Design	13.5.1 To simulate realistic adversarial attacks during any cyber security assessment, the threat scenario should be designed and based on challenging but plausible cyber	

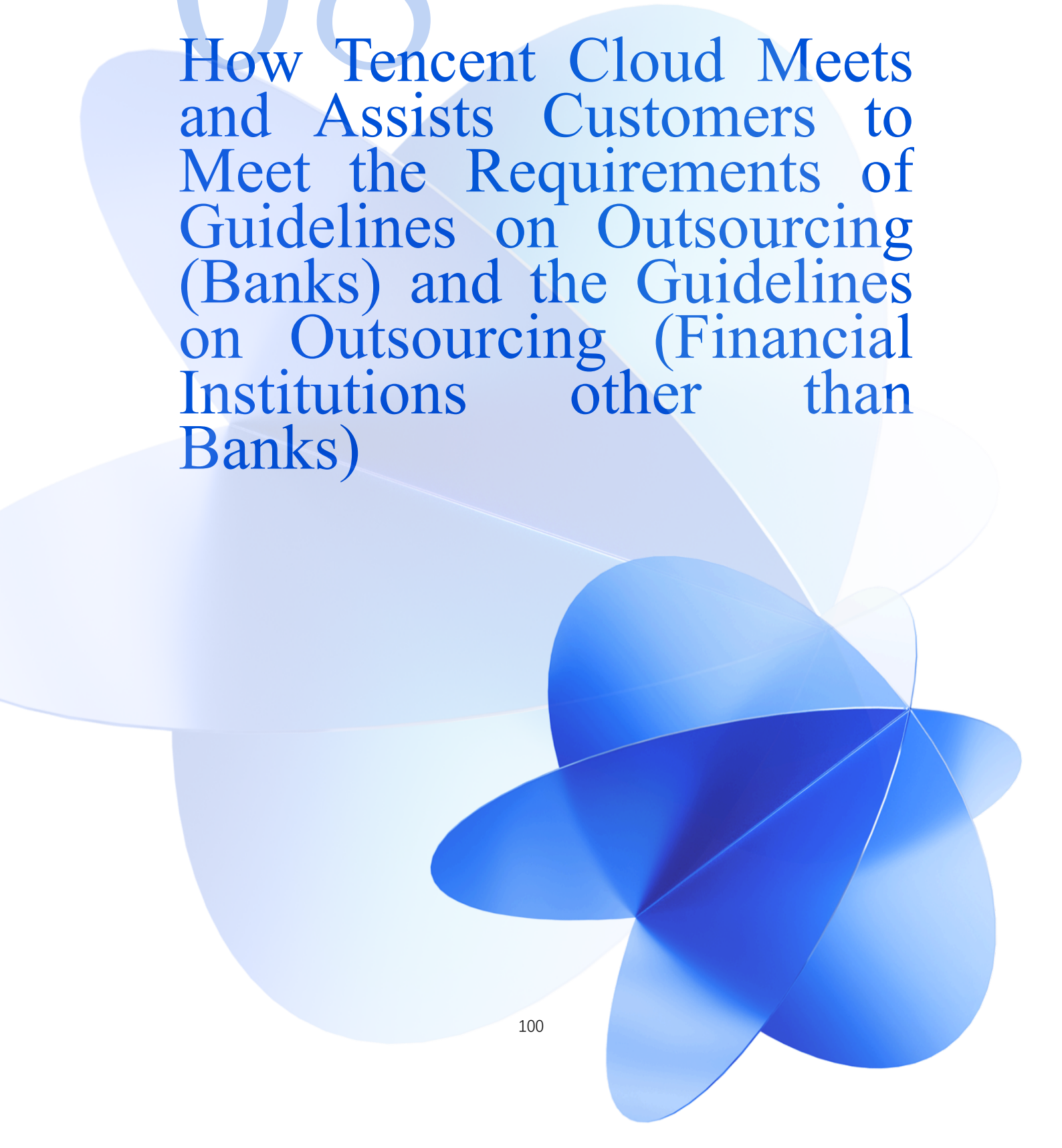
No.	Domain	Summary of Controls	Tencent Cloud's Response
		threats. 13.5.2 The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.	
13.6	Remediation Management	13.6.1 A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises. The process should minimally include the following: (a) severity assessment and classification of an issue; (b) timeframe to remediate issues of different severity; and (c) risk assessment and mitigation strategies to manage deviations from the framework.	Customers should establish a remediation process to track and resolve issues identified during cybersecurity assessments or drills. Tencent Cloud generates security vulnerability tickets for any vulnerabilities or deficiencies identified during security assessments or drills. These tickets are recorded in the security operations system and assigned to responsible personnel for remediation within a defined timeframe.

7.12 IT Audit

No.	Domain	Summary of Controls	Tencent Cloud's Response
15.1	Audit Function	15.1.1 The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls. 15.1.2 A comprehensive set of auditable areas for technology	Customers should establish an IT audit mechanism, conduct regular technology risk audits, and ensure that IT auditors possess the necessary professional competence and skills. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong

No.	Domain	Summary of Controls	Tencent Cloud's Response
		risk should be identified so that an effective risk assessment could be performed during audit planning. 15.1.3 The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process. 15.1.4 The FI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.	security posture in compliance with applicable laws, regulations, and security management standards. 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 cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Singapore financial regulations, Tencent Cloud engages third-party audit firms annually to perform independent audits of its internal control framework and issues the Outsourced Service Provider Audit Report (OSPAR) in accordance with the Singapore Bankers Association standards.

08 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions other than Banks)



The Monetary Authority of Singapore (MAS) has issued two separate guidelines: the Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions other than Banks). These guidelines set out MAS's expectations for banks and financial institutions that have entered into any outsourcing arrangements or plan to outsource their business activities to service providers.

Both guidelines focus on requirements related to outsourcing risk management measures, and their provisions are highly similar. Therefore, in this section, Tencent Cloud summarizes and consolidates the control requirements relevant to cloud service providers from both guidelines, and explains how Tencent Cloud, as a cloud service provider, assists banks and other financial institutions in meeting these requirements.

No.		Domain	Summary of Controls	Tencent Cloud's Response
Bank	Financial Institutions			
3.3.1	5.4.1	Assessment of service providers	In considering, renegotiating or renewing an outsourcing arrangement, banks and financial institutions should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.	When selecting a service provider, customers should conduct comprehensive due diligence. The assessment should focus on the provider's compliance capabilities and track record, physical and information technology security controls, business reputation, financial strength and resources, risk management framework and capabilities, disaster recovery arrangements. The due diligence process should be properly documented in writing. Where applicable, customers should supplement the assessment with on-site visits, independent reviews, and/or market feedback. Customers may incorporate the due diligence process into their outsourcing arrangement management framework and define the frequency and approach for periodic due diligence based on the nature and risk level of the outsourcing arrangement. In response to customer evaluations of service providers, Tencent Cloud will provide relevant information upon request and assign dedicated personnel to actively support and cooperate with customers' due diligence activities. Below is an overview of how Tencent Cloud, as a cloud service
3.3.2	5.4.2	Assessment of service providers	Banks and financial institutions shall assess various relevant factors of service providers, including their ability to exercise a high standard of care in performing the outsourcing arrangements to meet regulatory obligations, the physical and information technology security controls implemented, business reputation and financial strength, ethical and professional standards,	

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			and the capacity to fulfill all obligations under the outsourcing arrangements. On-site inspections of the service providers shall be conducted, and where possible, independent reviews and market feedback on the service providers shall be obtained to supplement the assessment by the financial institutions or banks.	provider, addresses each aspect of due diligence: • **Financial stability:** Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant.
3.3.3	5.4.3	Assessment of service providers	The due diligence should involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider′ s: (a) experience and capability to implement and support the outsourcing arrangement over the contracted period; (b) financial strength and resources; (c) corporate governance, business reputation and culture, compliance, and pending or potential litigation; (d) security and internal controls, audit coverage, reporting and monitoring	• **Business Reputation**: As the cloud computing brand under Tencent, a leading enterprise in China's internet industry, Tencent Cloud has obtained multiple professional certifications from industry authorities. It provides comprehensive cloud computing solutions and has partnered with over 11,000 companies to deliver more than 400 industry-specific solutions across 30+ sectors. • **Resources and Scale:** Tencent Cloud's operational capabilities and scale are among the leaders in the industry. Its data centers are deployed across multiple global regions, covering Mainland China, the Asia-Pacific region, North America, and Europe. • **Technical strengths**: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies,

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			environment; (e) risk management framework and capabilities; (f) disaster recovery arrangements and disaster recovery track record; (g) reliance on and success in dealing with sub-contractors; (h) insurance coverage; (i) external environment; and (j) ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.	global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products, ensuring reliable and continuous service for customers. • **Compliance Capability**: 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. The security team also performs ongoing internal and external audits of Tencent Cloud's security management system each year to ensure the effectiveness and compliance of its information security measures. • **Risk Management**: Tencent has established a risk governance framework and related procedures and continuously enhances its risk management measures and internal control systems. Tencent Cloud strengthens its risk culture to effectively improve internal risk management capabilities and ensure the healthy and sustainable development of its business. • **Business Continuity and Disaster**
3.3.5	5.4.5	Assessment of service providers	Due diligence undertaken during the assessment process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing arrangements. A risk-based approach may be used to determine the frequency for the re-performance of due diligence for outsourcing arrangements. The due diligence process may vary depending on the	

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			nature, and extent of risk of the arrangement and impact to the institution in the event of a disruption to service or breach of security and confidentiality. An institution should ensure that the information used for due diligence evaluation is sufficiently current. An institution should also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.	**Recovery**: Tencent Cloud has obtained ISO/IEC 22301 certification for its Business Continuity Management System. To ensure the continuous availability of customer services, Tencent Cloud has developed detailed disaster recovery plans for its cloud products and conducts regular drills in strict accordance with requirements to ensure the timeliness and feasibility of these plans.
3.3.4	5.4.4	Assessment of service providers	Banks and financial institutions should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the institution ' s hiring policies for the role they are performing, consistent with the criteria applicable to its own employees. The following are some non-exhaustive examples of what should be considered under this assessment: (a) whether they have been the subject of any proceedings of a	Customers should evaluate the employees engaged by the service provider for outsourced arrangements, paying attention to any disciplinary or compliance issues and financial status. Any adverse findings should be carefully considered to ensure that personnel meet the customer's hiring standards for the relevant positions. To support customers in meeting regulatory requirements, Tencent Cloud has established comprehensive human resource management standards and procedures to ensure recruitment and assignment of personnel according to job requirements. During the hiring process, Tencent Cloud reviews prospective employees, contractors, and third parties to assess their ability to meet position requirements. Subject to applicable laws and job level, the Human Resources department conducts pre-employment background checks, which include verification of past employment

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			disciplinary or criminal nature; (b) whether they have been convicted of any offence. (c) whether they have accepted civil liability for fraud or misrepresentation; and (d) whether they are financially sound. Any adverse findings from this assessment should be considered in light of their relevance and impact to the outsourcing arrangement.	history, criminal records, and academic qualifications. The results of these checks are recorded in Tencent Cloud's HR management system. Upon employment, internal staff sign employment and confidentiality agreements that clearly define Tencent Cloud's security policies, responsibilities of employees or third-party personnel, and potential penalties for violations. Outsourced personnel are also subject to pre-employment background checks and must comply with employment and confidentiality requirements stipulated in agreements between Tencent Cloud and the outsourcing vendor.
3.4.1	5.5.1	Outsourcing agreement	Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements. They should also be vetted by a competent authority (e.g. the institutions ' legal counsel) on their legality and enforceability.	Customers should enter into an outsourcing agreement with the service provider that covers the scope of the arrangement, performance and risk management standards, confidentiality and security obligations, business continuity, monitoring and control mechanisms, audit rights, notification of adverse events, dispute resolution, termination and early exit provisions, and applicable laws. The agreement must ensure legal validity and enforceability. Where the outsourcing service provider is located outside Singapore, the agreement should include additional provisions to mitigate cross-border outsourcing risks.

No.		Domain	Summary of Controls	Tencent Cloud's Response
Bank	Financial Institutions			
3.4.2 3.4.3 4.4.4 3.4.5	5.5.2	Outsourcing agreement	Banks and financial institutions should ensure that every outsourcing agreement addresses the risks identified at the risk evaluation and due diligence stages. Each outsourcing agreement should allow for timely renegotiation and renewal to enable the institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations. It should at the very least, have provisions to address the following aspects of outsourcing: (a) scope of the outsourcing arrangement; (b) performance, operational, internal control and risk management standards; (c) confidentiality and security; (d) business continuity management; (e) monitoring and control; (f) audit and inspection; (g) notification of adverse developments; (h) dispute resolution; (i) default termination and	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 set out 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 termination scenarios, the dispute-resolution mechanism, and the notice procedure. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. In addition, **if customers need to terminate the contractual agreement due to business changes or future IT planning**, they may choose to back up and migrate cloud data and production environments at any time. Tencent Cloud supports customers in backing up or migrating data using common standard formats. This enables customers to adopt the same transmission methods and protocols used during cloud onboarding, or leverage network services such as **Direct Connect (DC)**and **VPN Connection** to ensure secure and reliable data transfer during termination of cloud service engagement.

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			early exit: including scenarios where banks and financial institutions have the right to terminate the outsourcing agreement, the clearly specified minimum period required to implement the termination clauses, and other relevant provisions to ensure a smooth transition upon the termination or amendment of the agreement; (k) applicable laws.	
3.4.8	5.5.3	Outsourcing agreement	Each agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore.	
3.4.7	N/A	Outsourcing agreement	Upon termination of the outsourcing arrangement, banks shall make every reasonable effort to ensure that the information provided by them to the service provider—including customer information and non-customer information—is deleted, destroyed, or rendered	Customers should ensure that, upon termination of outsourcing, all information provided to the service provided, including customer and non-customer information—is deleted or destroyed, unless retention is justified based on an assessment by the bank. **For data deletion and destruction**, Tencent Cloud provides secure and reliable data erasure mechanisms. Upon service termination, Tencent Cloud apply strict data

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			unusable, unless the bank determines through assessment that the service provider has a legitimate reason to retain such non-customer information.	erasure procedures. After the retention period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable.
3.5.1 3.5.3 3.5.4	5.5.2(j)	Use of Subcontractors	When service providers engage subcontractors, banks and financial institutions should retain the ability to monitor and control their outsourcing arrangements. The outsourcing agreement shall contain clauses on rules and restrictions regarding subcontracting. Banks and financial institutions should ensure that if any part of a material outsourcing arrangement is to be subcontracted, they must be notified and give their approval, and the notification to the bank shall be completed no later than 30 days in advance. In addition, banks shall take reasonable measures to ensure that subcontractors comply with the same or similar standards as the primary service providers, including confidentiality obligations, information access controls, and	Customers should clearly define rules, restrictions, and relevant standards for subcontracting in the outsourcing agreement, and ensure that the service provider notifies and obtains approval before engaging any subcontractor. Tencent Cloud publishes the online **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, and other legal documents on its international portal. For sub-processing scenarios, these agreements expressly set out clauses on prior consent to sub-processing, advance notice of any addition or replacement of sub-processors, and data-protection obligations. Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the relevant contract/agreement without the customer's prior written consent. Any anticipated change involving the addition or replacement of a sub-processor will be notified to the customer by e-mail or other agreed channels. Customers may also elect to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Regarding sub-contractor management, Tencent Cloud maintains a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			restrictions on information disclosure. This can be achieved by incorporating appropriate clauses into the outsourcing agreement signed with the service provider.	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 the Monetary Authority of Singapore and financial institutions. In addition, Tencent Cloud actively cooperates with customers' outsourcing-management requirements and responds to and participates in audits or assessments initiated by customers.
3.6.1	5.6.1	Confidentiality and Security	it is vital that banks and institutions satisfies itself that the service provider ' s security policies, procedures and controls will enable the institution to protect the confidentiality and security of customer information.	Customers should ensure, through outsourcing agreements, restrictions on information disclosure, and review and monitoring mechanisms, that the service provider's security policies, procedures, and controls effectively protect the confidentiality and security of customer information. **From a compliance perspective**, Tencent Cloud strictly adheres to laws and regulations governing user privacy and data security in the jurisdictions where it operates. It has established a comprehensive information security and privacy protection management system and obtained multiple international certifications. Tencent Cloud follows the principle of "data confidentiality" by implementing security mechanisms such as virtualization control layer resource access policies, internal private network isolation strategies within the cloud platform, permission allocation and identity authentication for the web console, and session IDs and access keys for APIs. These
3.6.2	5.6.2	Confidentiality and Security	Banks and financial institutions should take the following steps to protect the confidentiality and security of customer information: (a)State the responsibilities of contracting parties in the outsourcing agreement, including the circumstances under which each party has the	

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			right to change security requirements. The outsourcing agreement should also address: the issue of the party liable for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the institution; and the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of contracted service; (b) Disclose customer information to the service provider only on a need-to-know basis; (c) Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets, particularly where multi-tenancy arrangements are present at the service provider; and (d) Review and monitor the security practices and control processes of the	measures ensure data isolation between customers, preventing tenants from accessing, obtaining, or tampering with other tenants' data. Tencent Cloud also provides services such as **Virtual Private Cloud (VPC)** and **Cloud Firewall (CFW)** to help customers further strengthen network isolation and perimeter protection. In addition, many Tencent Cloud storage and database products support data encryption using secure, high-strength algorithms, and integrate with the **Key Management Service (KMS)** to enable full lifecycle management of encryption keys, ensuring the confidentiality of customer information. **Regarding customer data protection**, Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with national laws and regulations during investigations by government authorities. Tencent Cloud enforces access control and permission management and requires employees to sign confidentiality agreements to safeguard customer data. Tencent Cloud also provides online legal documents such as the **Terms of Service** 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

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the institution breaches of confidentiality in relation to customer information.	both customers and Tencent Cloud. For more details on confidentiality and security measures, please refer to Section 5.1 : "**7.1 & 7.2 Outsourcing Agreements and Information Access for Material Ongoing Outsourcing**" and "**8.1 Customer Information Protection for Material Ongoing Outsourcing**." In addition, Tencent Cloud actively supports and cooperates with customer **audits and reviews**, providing dedicated personnel for assistance.
3.7.1	5.7.1	Business Continuity Management	Banks and financial institutions should ensure that its business continuity is not compromised by outsourcing arrangements, it should adopt the sound practices and standards contained in the BCM Guidelines, in evaluating the impact of outsourcing on its risk profile and for effective BCM.	Customer shall assess the impact of any outsourcing arrangement on its risk profile and implement measures to mitigate risks arising from such arrangements. These measures include but are not limited to: executing a written agreement, verifying the service provider's business continuity plan (BCP) and related testing or exercises, establishing termination procedures for the outsourcing arrangement, initiating joint drills, and developing feasible alternatives for operational recovery. The objective is to ensure that outsourcing does not compromise the Customer's business continuity. **To ensure the continuous stability and availability of Customer operations**, Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options to meet disaster recovery and service level requirements. Tencent Cloud's
3.7.2	5.7.2	Business Continuity Management	In line with the BCM Guidelines, an institution should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated These should include taking the	

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			following steps: (a) Incorporate the necessary contractual requirements and verify that the service provider has in place satisfactory business continuity plans (BCP) that are commensurate with the nature, scope and complexity of the outsourcing arrangement; (b) Proactively seek assurance on the state of BCP preparedness of the service provider. It should ensure the service provider regularly tests its BCP to ascertain that the recovery objectives can be met. The institution should require the service provider to notify it of any test finding that may affect the service provider's performance. The institution should also require the service provider to notify it of any substantial changes in the service provider's BCP and of any adverse development that could substantially impact the service provided to the institution; and (c) Ensure that there are	compute, network, storage, database, container, middleware, and security services are designed for high availability and supported by corresponding disaster recovery plans. Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console. In terms of business continuity management, Tencent Cloud is certified under the ISO/IEC 22301 international standard and has established a comprehensive internal business continuity management system, including regular disaster recovery drills and tests. These drills often simulate real-world disaster scenarios, such as attack-defense exercises and large-scale failures, to thoroughly validate system resilience, response speed, and recovery capability. For more details on business continuity, refer to Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management." **If the Customer elects to terminate or exit cloud services**, the Customer may back up and migrate data and production environments at any time. Tencent Cloud supports standard formats for data backup and migration. Upon termination of

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement and that all documents, records of transactions and information previously given to the service provider should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.	services, Tencent Cloud will permanently delete Customer data following strict data erasure procedures after the retention period expires. Deleted data cannot be recovered. Tencent Cloud provides multiple communication channels, including the console, official website, and email, to fulfill notification and communication obligations. For more details on notifications and communication, refer to Section 7.5 : "**7.7 Incident Management**." Tencent Cloud will actively respond to Customer-initiated assessments or audits and provide dedicated support as required.
3.7.3	5.7.3	Business Continuity Management	Banks and financial institutions should involve its service providers, where applicable, in the validation and testing of its BCP. Similarly, an institution could take part in its service providers ′ business continuity and disaster recovery tests.	
3.7.4	5.7.4	Business Continuity Management	Banks and financial institutions should consider worst case scenarios in developing its BCPs for its outsourcing arrangements. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate	

No.		Domain	Summary of Controls	Tencent Cloud's Response
Bank	Financial Institutions			
			interdependency risk.	
3.8.1	5.8.1	Business Continuity Management	Banks and financial institutions should establish a structure for the management and control of its outsourcing arrangements. Banks and financial institutions should ensure that outsourcing agreements with service providers contain clauses to address the institution′ s monitoring and control of outsourcing arrangements.	Customer shall establish mechanisms for monitoring and managing outsourcing activities and shall ensure that monitoring and control provisions are clearly defined in the outsourcing agreement with the service provider. The Customer shall implement monitoring and control measures for all material outsourcing arrangements, including but not limited to: maintaining an outsourcing register, establishing an organizational structure for outsourcing management, conducting regular reviews of outsourcing arrangements, and promptly reporting any significant outsourcing-related incidents.
3.8.2	5.8.2	Business Continuity Management	Banks and financial institutions should take measures to achieve effective monitoring and control of any material outsourcing arrangements, including: establishing and maintaining a register of outsourcing arrangements; forming a cross-functional outsourcing management team; setting up an outsourcing management control group; conducting regular reviews of all material outsourcing arrangements at least	**To support the Customer's outsourcing monitoring requirements**, Tencent Cloud continuously tracks the performance and availability of each cloud service. Relevant metrics are available for real-time monitoring through the management console. Cloud services provided by Tencent Cloud are delivered in accordance with the Service Level Agreement (SLA) applicable to each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the Tencent Cloud official website. In addition, Tencent Cloud will cooperate with the Customer's third-party security audits and supervision in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities.

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			annually; performing comprehensive reviews before and after the implementation of new outsourcing arrangements or when modifying existing ones; conducting renewed due diligence if there are substantial changes to the outsourcing arrangements; ensuring that their monitoring indicators and performance data are not aggregated with similar data of other customers of the service providers; and ensuring that any material adverse developments arising in any outsourcing arrangement are promptly brought to the attention of the senior management of the banks/financial institutions and the service providers.	Tencent Cloud has established policies and procedures to define escalation standards for security incidents and maintains an incident escalation mechanism to ensure timely notification to affected parties when potential adverse events may impact the Customer's business. Reported security incidents are continuously tracked and managed until resolution. For more details on incident management and notifications, refer to Section 7.5 : "**7.7 Incident Management**."
3.9.2	5.9.2	Audit and inspection	Banks and financial institutions should include clauses in all outsourcing agreements involving material outsourcing arrangements that permit the banks/financial institutions to audit the service providers and their subcontractors.	The Customer shall ensure that all outsourcing agreements involving material outsourcing arrangements include provisions granting the Customer the right to audit and the right to obtain relevant audit reports from the service provider. For financial institution Customers, agreements with service providers involved in material outsourcing arrangements shall also include provisions granting the Monetary Authority of Singapore (MAS) the right to audit and

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			They shall also obtain copies of any reports and audit results related to the outsourcing arrangement from the service providers and their subcontractors. For financial institutions, material outsourcing agreements shall further contain relevant clauses to allow MAS or any agent appointed by it to exercise the institution's contractual rights when necessary or appropriate, including accessing and inspecting the relevant premises of the service providers and their subcontractors, obtaining documents and information provided by the institution to the service providers and their subcontractors, and acquiring any audit reports or findings related to the outsourcing arrangement.	requiring the service provider to promptly comply with any requirements from the institution or MAS. As a cloud service provider, 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. 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. 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.
N/A	5.9.3	Audit and inspection	Outsourcing agreements for material outsourcing arrangements should also include clauses that require the service provider to comply, as soon as possible, with any request from MAS or the institution to the	Tencent Cloud will cooperate with the Customer's third-party security audits and supervisory reviews in accordance with

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			service provider or its sub-contractors, to submit any reports on the security and control environment of the service provider and its sub-contractors to MAS.	applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. Tencent Cloud also undergoes regular independent third-party audits and provides assurance reports on system and organizational controls to cloud users, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud services.
3.9.3	5.9.4	Audit and inspection	Banks and financial institutions should ensure that any subcontractors engaged by service providers in delivering services related to material outsourcing arrangements comply with the audit requirements and expectations applicable to such service providers. MAS will endeavor to provide the institution reasonable notice of MAS' intent to exercise its inspection rights and share its findings with the institution where appropriate.	To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet Singapore financial regulatory requirements, Tencent Cloud engages an independent audit firm annually to perform an audit of its internal control framework and issue the Outsourced Service Provider Audit Report (OSPAR) under the Association of Banks in Singapore (ABS) guidelines. Tencent Cloud also exercises effective control over its subcontractors through rigorous security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements. These measures ensure that subcontracting does not impair Tencent Cloud's ability to provide relevant services to customers, the confidentiality and integrity of customer information processing, or the supervisory and audit rights of the Monetary Authority of Singapore (MAS) and financial institutions.

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
3.9.4	5.9.5	Audit and inspection	Banks and financial institutions should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the institution should consider the nature and extent of risk and impact to the institution from the outsourcing arrangements. The scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security and control environment incident management process and the institution's observance of the expectations in these Guidelines in relation to the outsourcing arrangement.	The Customer shall conduct independent audits and/or expert assessments of all service providers and their subcontractors involved in material outsourcing arrangements on a regular basis. Personnel performing such audits or assessments shall possess the necessary professional knowledge, skills, and independence. The scope of the audit or assessment shall include, at a minimum, the security and control environment of the service provider and its subcontractors, as well as incident management processes. The Customer shall promptly implement corrective actions for any issues identified during audits or assessments and verify the adequacy of remediation measures taken by the service provider. **To facilitate the Customer's audit and review requirements**, Tencent Cloud will provide dedicated assistance and actively cooperate with Customer-initiated audit or review activities. Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes regular independent third-party audits and assessments. Through these audits, Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications. Based on Customer requirements, Tencent Cloud provides assurance reports on system and organizational controls to cloud users, independent auditors, regulators, shareholders, and other stakeholders,
3.9.5	5.9.6	Audit and inspection	The independent audit and/or expert assessment on the service provider and its sub-contractors may be performed by the Banks or institution's internal or external auditors, the service provider's external	

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			auditors or by agents appointed by the institution. The appointed persons should possess the requisite knowledge and skills to perform the audit, and be independent of the unit or function performing the outsourcing arrangement. Senior management should ensure that appropriate and timely remedial actions are taken to address the audit findings. Institutions and the service providers should have adequate processes in place to ensure that remedial actions are satisfactorily completed. Actions taken by the service provider to address the audit findings should be appropriately validated by the Banks or institution before closure.	disclosing the latest internal control status of Tencent Cloud services. In Singapore, Tencent Cloud complies with local information security and personal data protection requirements and has obtained the Data Protection Trustmark (DPTM) certification and Multi-Tier Cloud Security (MTCS) Tier 3 certification and Cyber Trust Mark. Additionally, Tencent Cloud engages audit firms with extensive experience in the Singapore financial industry to perform annual independent audits of Tencent Cloud's management systems and maintain the Outsourced Service Provider Audit Report (OSPAR) under the Association of Banks in Singapore (ABS) guidelines. **For any issues identified during audits or assessments**, Tencent Cloud will evaluate the potential impact on the Customer, perform root cause analysis, and implement appropriate corrective measures. If such issues may affect the operations or data security of financial institutions, Tencent Cloud will promptly notify the relevant institutions. Management will track and monitor the execution of remediation plans and actions on an ongoing basis to ensure effective resolution.
3.9.6	5.9.7	Audit and inspection	Significant issues and concerns should be brought to the attention of the senior management of the Banks or institution and service provider, or to the institution′ s board, where warranted, on a	Tencent Cloud has established an information security management policy to support secure cloud operations and risk management. Leveraging advanced cloud computing technologies, robust cybersecurity capabilities, global data center infrastructure, and industry-specific solutions, Tencent Cloud provides comprehensive security protection throughout the data lifecycle and ensures a

No.		Domain	Summary of Controls	Tencent Cloud's Response
Bank	Financial Institutions			
			timely basis. Actions should be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the Banks or institution ′ s risk tolerance.	secure and reliable cloud computing environment. For more details on security and control environment, refer to Section 7.1: "Technology Risk Governance and Oversight." For security incidents that may impact the Customer, Tencent Cloud will, after internal review, communicate the handling and analysis results through appropriate channels based on the scope and severity of the incident.
3.9.8	N/A	Audit and inspection	Audits and/or expert assessments conducted as part of the certification process may be used to meet the audit requirements or expectations, provided that such audits or assessments are performed by independent and competent auditors. Banks shall confirm that the scope and methodology of the audits enable them to clearly determine the service providers' ability to perform the outsourcing arrangements, as well as the adequacy of the service providers' risk management frameworks and capabilities.	
3.10.1	5.10.1	Outsourcing outside Singapore	The engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in	When engaging overseas service providers, the Customer shall, based on due diligence, continuously consider factors such as government policies, political and social environment, foreign laws and regulations, regulatory oversight, supervision of the

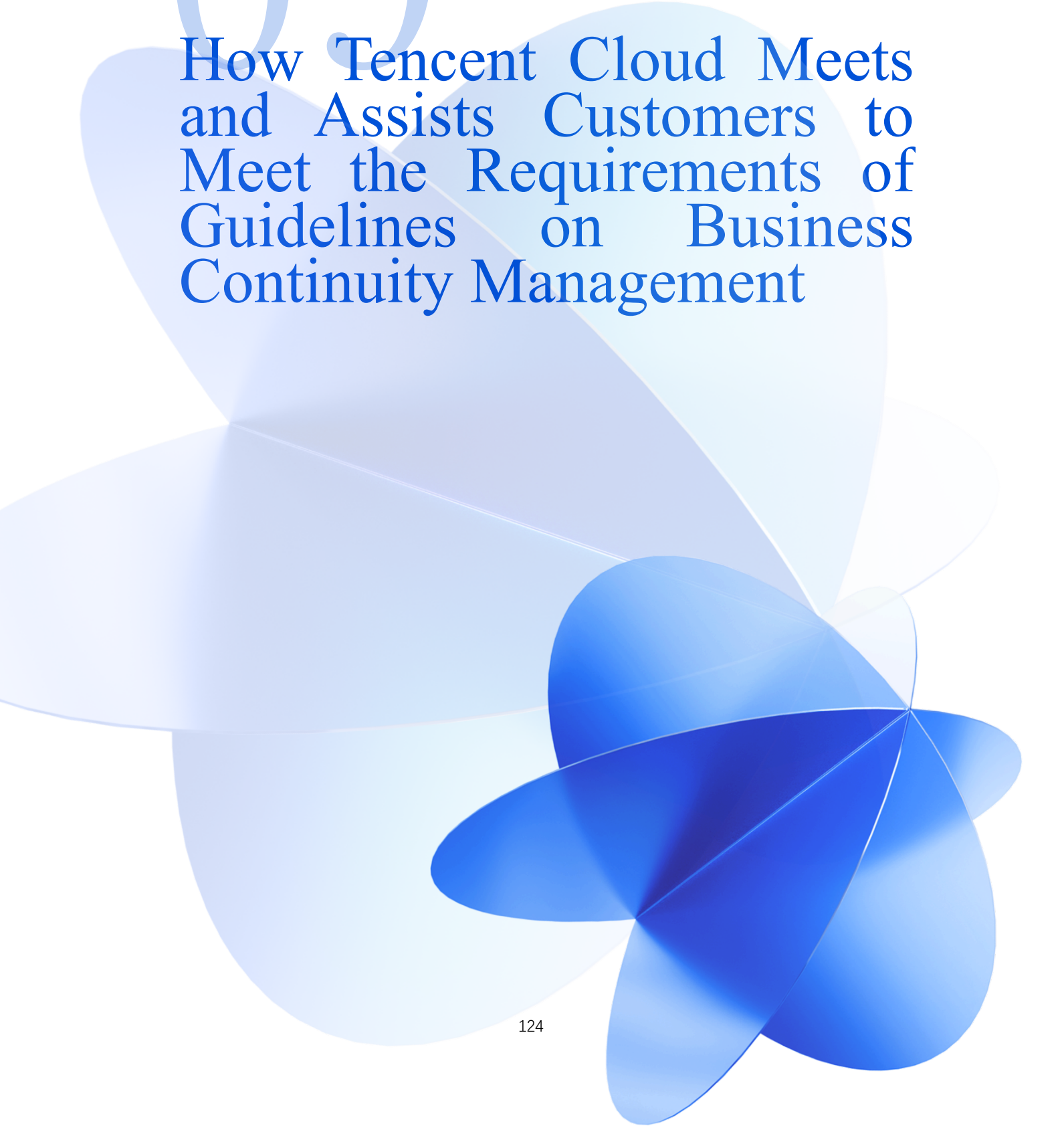
No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			a foreign country, an institution should take into account, as part of its due diligence, and on a continuous basis: (a) government policies; (b) political, social, economic conditions; (c) legal and regulatory developments in the foreign country; and (d) the institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy. An institution should also be aware of the disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. As information and data could be moved to primary or backup sites located in foreign countries, the risks associated with the medium of transport, be it physical or electronic, should also be considered.	service provider, exit strategies, and business continuity management. The Customer shall also understand the service provider's disaster recovery arrangements and related locations, as well as data transmission protection measures. The Customer shall ensure that overseas outsourcing does not impede the Monetary Authority of Singapore (MAS) in supervising the Customer's business activities in Singapore. **To meet Customer requirements for business continuity and data localization**, Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options and strictly complies with applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Customers may flexibly deploy data and systems across different regions or availability zones based on business needs and data security requirements. Currently, Tencent Cloud operates four data centers in Singapore, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Singapore-based Customers may choose to store and process their data locally within Singapore. **To ensure continuous availability of Customer operations**, Tencent Cloud's compute, network, storage, database, container, middleware, and security

No.		Domain	Summary of Controls	Tencent Cloud's Response
Bank	Financial Institutions			
3.10.2	5.10.2	Outsourcing outside Singapore	Material outsourcing arrangements with service providers located outside Singapore should be conducted in a manner so as not to hinder MAS′ efforts to supervise the Singapore business activities of the institution in a timely manner, in particular: (a) An institution should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements. (b) It should not enter into outsourcing arrangements with service providers located in jurisdictions where legal or administrative restrictions may impede MAS or its designated agents from obtaining timely access to the service providers' information.. For Financial institutions, It should notify MAS if any overseas authority were to seek access to its customer information or if a situation were to	services are designed for high availability and supported by disaster recovery plans. Tencent Cloud has established a comprehensive internal business continuity management system and is certified under the ISO/IEC 22301 international standard for business continuity management. **Regarding data access and protection,** Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud adheres to the principle of "data privacy" and will not access Customer data unless required for service delivery or troubleshooting, and only with explicit Customer authorization or as required by national or local authorities for lawful investigations. All communications through the Tencent Cloud console are encrypted using HTTPS. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. **In terms of contracts/agreements,** 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... **If the Customer elects to terminate or exit cloud services**, the Customer may

No. Bank	No. Financial Institutions	Domain	Summary of Controls	Tencent Cloud's Response
			arise where the rights of access of the institution and MAS, have been restricted or denied.	back up and migrate data and production environments at any time. Tencent Cloud supports standard formats for data backup and migration. Upon termination of services, Tencent Cloud will, in accordance with the service agreement, permanently delete Customer data, including copies and backups, following strict data erasure procedures after the retention period expires. Deleted data cannot be recovered.
Annex 2	Annex 5	Cloud Computing	7.Banks and Institutions should be aware of CS′ typical characteristics and take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, Banks and institutions should ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls. The service provider should have in place robust access controls to protect customer information and such access controls should survive the tenure of the contract of the CS.	The Customer shall consider, and address risks associated with typical cloud computing characteristics, particularly data isolation and access protection. Customer data is classified as a high-security-level data within Tencent Cloud. Customer data within Tencent Cloud remains under the Customer's sole ownership and control. Tencent Cloud enforces strict isolation through virtualization resource access control policies, internal private network segmentation, web console permission management and authentication, session ID and access key mechanisms, ensuring that tenants cannot access, obtain, or modify other tenants' data. For more details on data isolation, data protection, and cloud security, refer to Section 10 "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption".

09

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management



The Monetary Authority of Singapore (MAS) has issued the Guidelines on Business Continuity Management to provide guidance for Financial Institutions (FIs) on establishing a robust business continuity management framework and implementing relevant controls. The purpose of these guidelines is to enhance operational resilience and minimize the impact of disruptions on the ability of FIs to deliver financial services continuously. The requirements under the guidelines primarily address areas such as critical business services and functions, recovery time objectives, dependency mapping, concentration risk, continuous review and improvement, testing, audit, incident management, and crisis management.

In response to these requirements, Tencent Cloud has designed and implemented a business continuity management framework tailored to its cloud computing environment. Tencent Cloud has established a comprehensive business continuity management system, formalized policies and procedures, and standardized processes that cover business impact analysis, business continuity planning, emergency response and disaster recovery, emergency drills and testing, and crisis management. Tencent Cloud has also obtained ISO/IEC 22301 certification for its business continuity management system, demonstrating compliance with international standards.

This section summarizes the control requirements in the Guidelines on Business Continuity Management that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists Financial Institutions in meeting these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers should determine the priority of business recovery, recovery strategies, and resource allocation based on the criticality of business services and functions. To support the Customer in meeting regulatory requirements, Tencent Cloud conducts business impact analysis for its cloud products and services in accordance with its internal business continuity management policies. This analysis includes identifying critical products and services, mapping activities that support service delivery, assessing the impact of disruptions over time, establishing recovery priority timelines at the minimum acceptable level, identifying dependencies and supporting resources, and formulating appropriate response strategies based on the analysis results.
2.2	Critical Business Services and Functions	The FI should therefore prioritize the recovery of its business services and functions based on their criticality, and determine the appropriate recovery strategies and resource allocation.	
3.1	Service Recovery Time Objective	The FI should establish a Service Recovery Time Objective (SRTO) for each critical business service. The SRTO, being a time-based	Customers should set a Service Recovery Time Objective (SRTO) for each critical business service and develop corresponding recovery strategies to ensure the achievement of the SRTO. For critical business services supported

No.	Domain	Summary of Controls	Tencent Cloud's Response
		metric, provides clarity within the FI on the expected recovery timelines for each business service.	by multiple business functions, the underlying business functions and their dependencies must have Recovery Time Objectives (RTOs) that meet the SRTO requirements. To ensure continuous availability of Customer operations, Tencent Cloud performs business impact analysis for its cloud products and services, defines RTOs and Recovery Point Objectives (RPOs), and develops response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans are established for cloud products and critical processes, covering facilities, personnel, equipment, systems, information and data, and business priorities. Tencent Cloud regularly conducts business continuity drills and tests based on these plans to ensure their feasibility.
3.2	Service Recovery Time Objective	In establishing SRTOs, the FI should take into consideration its obligations to customers, as well as other FIs that depend on the business services. The FI is expected to put in place recovery strategies6 to enable it to achieve the established SRTOs and recover to the service levels required to meet its business obligations. For critical business services that are supported by a number of business functions, the FI must ensure that the Recovery Time Objectives (RTOs) of the underlying business functions and their dependencies will meet the SRTOs.	
3.3	Service Recovery Time Objective	The FI should also set out clearly defined criteria for BCP activation when a critical business service encounters partial disruption (including intermittent or reduced performance that is not tantamount to a complete unavailability of service).	Customers should establish clear criteria for activating the Business Continuity Plan (BCP) to control the scope of impact before service performance deteriorates and causes severe consequences. To support regulatory compliance, Tencent Cloud has defined procedures for incident monitoring and reporting, emergency response, disaster recovery, and crisis management within its internal business continuity management framework. Tencent Cloud aims to minimize the adverse impact of unexpected events in the shortest possible time. Through its incident alert system, Tencent Cloud reports, analyzes, and classifies incidents, and initiates recovery actions based on the severity level and corresponding recovery time requirements and response strategies, thereby reducing or

No.	Domain	Summary of Controls	Tencent Cloud's Response
			preventing operational disruptions that could affect asset security and business operations.
4.4	Third-Party Dependencies	The FI should put in place measures that enable third parties to meet the SRTOs of its critical business services. This can be done through measures, such as the following: establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations; review the BCPs of third parties and verify that the BCPs meet appropriate standards and are regularly tested. establish arrangements with third parties to safeguard the availability of resources,; conduct audits on the third parties; or perform joint tests with third parties.	Customers should take appropriate measures to ensure that third-party service providers are able to meet the Service Recovery Time Objectives (SRTO) for critical business services. Tencent Cloud offers a wide range of products designed with high availability features to help customers achieve system and service resilience. For example: • **Cloud Load Balancer (CLB)** 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. • **Cloud Virtual Machine (CVM)** 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. • **Cloud Object Storage (COS)** provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • **Cloud Native Database TDSQL-C** adopts a high-availability cluster architecture capable of automatically detecting node failures and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			supporting second-level failover and recovery. • TencentDB for MySQL supports high reliability and availability with robust automatic backup and lossless recovery mechanisms. • Tencent Kubernetes Engine (TKE) 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. Tencent Cloud delivers its cloud services in accordance with the agreed Service Level Agreements (SLAs). The performance indicators, measurement standards, and reporting requirements for each service are clearly defined in the SLA for the respective product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of its cloud services and provides real-time monitoring capabilities to Customers through the management console. In addition, Tencent Cloud offers dedicated support and actively responds to Customer-initiated audits or review activities to facilitate compliance and oversight.
4.5	Third-Party Dependencies	The FI should also put in place plans and procedures to address any unforeseen disruption, failure or termination of third-party arrangements to minimize the impact of such adverse events on the continuity of its critical business services.	Customers shall develop plans and procedures to address any unforeseen interruption, failure, or termination of third-party arrangements. To ensure continuous availability of Customer operations, Tencent Cloud provides a wide range of cloud products and services—including computer, network, storage, database, container, middleware, and security services—all designed with high availability and supported by disaster recovery plans. Tencent Cloud builds or leases data centers in multiple global locations in compliance with relevant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			international standards and local security requirements, offering Customers multi-region and multi-availability zone options to meet disaster recovery and service level requirements. Tencent Cloud has established a comprehensive internal business continuity management system, obtained ISO/IEC 22301 certification, and conducted regular disaster recovery drills and tests to validate system resilience, response speed, and recovery capability.
4.6	Third-Party Dependencies	The FI should put in place measures to address the disruption of common utility services supporting critical business services (such as telecommunications networks and electricity utilities), such as implementing redundancy or alternative contingency arrangements.	Customers should also implement measures to address interruptions in utility services supporting critical business operations, such as public power supply and telecommunications networks. To support regulatory compliance, Tencent Cloud connects each availability zone to multiple network carriers, enabling cross-region network redundancy and reducing the impact of carrier-level outages. Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures. Similarly, Tencent Cloud's compute nodes adopt redundancy, and any faulty node is automatically removed by the scheduler in real time, ensuring service continuity for Customer workloads. Tencent Cloud's global data centers are selected, constructed, or leased in accordance with international standards and local security requirements. In Singapore, Tencent Cloud operates four leased data centers and requires data center operators to implement fully redundant, high-stability power systems to prevent single-point failures from affecting continuous power supply.

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.2	Concentration Risk	The FI could consider adopting the following approaches to mitigate the risk of concentration and reduce the impact in the event of disruption: primary-secondary site operation – separate primary and secondary sites of critical business services and functions, or infrastructure (such as data centers) into different zones to mitigate wide-area disruption. critical business functions segregation – separate critical business functions into different zones to mitigate the risk of losing multiple critical business functions, and the critical business services that they support, from a wide area disruption; split team and back-up team arrangements – deploying critical personnel across different zones, or establish reserve team arrangements13 to eliminate the dependency on a single labor pool; cross-training – identify critical skills or roles and develop cross-training programs to build versatility for key personnel involved in these roles. cross-border support – activate cross-border support as a contingency during disruptions; or alternative service provider – engage an alternate service provider for redundancy, or to be	The Customer shall take measures to mitigate concentration risk and reduce its impact in the event of disruption. **To assist Customers in addressing concentration risk**, Tencent Cloud operates data centers across multiple global regions, organized into regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. When launching instances, customers can select any Availability Zone within a designated Region deploying instances across independent Availability Zones safeguards applications against failures in a single location. Customers can flexibly deploy data and systems across different regions or availability zones according to business development needs and data security requirements, adopting suitable business continuity models to meet disaster recovery objectives. Tencent Cloud also provides **Cloud Load Balancer (CLB)** to enhance the availability of Customer application systems. CLB offers secure and efficient Layer 4 and Layer 7 traffic distribution services, enabling horizontal scaling of application systems, eliminating single points of failure, and ensuring service continuity through cluster-based deployment that automatically removes faulty instances. In addition, **Tencent Cloud offers multiple storage and database services with built-in backup capabilities**, supporting multi-redundant backups and cross-region disaster recovery. • **Cloud Object Storage (COS)**: 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		activated to provide immediate support when the primary service provider is unavailable.	• Cloud Block Storage (CBS): 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. • Cloud Native Database TDSQL-C: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • TencentDB for MySQL: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • TencentDB for MongoDB: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios. **From a personnel perspective**, Tencent Cloud defines roles and responsibilities for recovery processes and implements an A/B role redundancy mechanism for critical skills and positions. Regular emergency drills and training are conducted to ensure rapid and effective execution of recovery procedures, supporting Customers in achieving timely restoration during business disruption scenarios.
6.3	Threat Monitoring, Review and Reporting	The FI should actively monitor and identify external threats and developments that could disrupt its normal operation, and have an escalation process to alert internal stakeholders and senior management about the relevant threats in a timely manner.	Financial Institutions shall actively monitor and identify external threats, developments, and risks that may disrupt their normal operations, and establish internal processes for threat reporting and escalation. To support customers in threat detection and analysis, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.4	Threat Monitoring, Review and Reporting	The FI should institute processes to conduct environmental scanning for relevant risk events, such as natural disasters, terrorism, pandemic outbreaks, and cyber incidents. FIs should also monitor public advisories issued by relevant authorities to obtain the latest information and guidance on emerging threats that may pose a risk to their business continuity.	intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. TIX is SaaS-based and supports multiple delivery methods, including web portals, APIs, SDKs, TIP integration, and mini-programs, meeting varied customer needs. It can also integrate with customers' existing security products to enhance overall security operations and threat response efficiency. Empowered by TIX, Tencent Cloud aims to build a proactive defence capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable.
6.5	On-going Improvement	The FI should perform a review to identify areas of improvement and address any gaps in its BCM measures following an operational disruption. The FI should also draw lessons learnt from its own near misses, as well as incidents in other organizations, to enhance its	Following an operational disruption, the Customer shall review and improve its business continuity management measures and incorporate lessons learned from its own incidents or those of other organizations to strengthen its state of preparedness. To support regulatory compliance, Tencent Cloud has established continuous improvement

No.	Domain	Summary of Controls	Tencent Cloud's Response
		business continuity preparedness.	procedures and mechanisms that define corrective, preventive, and improvement actions after an incident occurs. Tencent Cloud analyzes the actual or potential causes of incidents or issues, evaluates the need for corrective and preventive measures, identifies improvement opportunities, and implements approved actions. For incidents that result in operational disruption, Tencent Cloud's quality management department organizes a post-incident review with the responsible teams, summarizes lessons learned, and issues an incident investigation report. The quality management department monitors the implementation of subsequent improvements to prevent recurrence of similar incidents.
6.6	On-going Improvement	The FI should regularly assess the need for additional tools and automation to enable it to manage an incident or disruption more effectively.	Customer shall assess and update its business continuity management strategies, plans, procedures, and measures, including relevant tools and automation capabilities, and regularly review its critical business services and functions, their Service Recovery Time Objectives (SRTO), Recovery Time Objectives (RTO), and dependencies.
6.7	On-going Improvement	The FI should update its BCM policies, plans, and procedures, including relevant training programmes for staff and test plans, based on changes in its operational environment and the threat landscape. The FI should also review its critical business services and functions, their respective SRTOs/ RTOs and dependencies at least annually, or whenever there are material changes that affect them.	To support regulatory compliance, Tencent Cloud conducts an annual assessment of the completeness, adequacy, and effectiveness of its business continuity management system and revises the system based on the assessment results. Tencent Cloud also reviews its business continuity plans annually and updates them as necessary. When significant changes occur in business functions or critical resources, Tencent Cloud reviews the scope of critical services and their component dependencies and promptly revises the business continuity plans. Customers regularly test its response and recovery arrangements for disruption scenarios, selecting appropriate test types based on the importance of critical business services and functions. All test activities shall be fully documented, and any gaps or weaknesses

No.	Domain	Summary of Controls	Tencent Cloud's Response
			identified during testing shall be reported, addressed, and tracked to completion. These measures ensure that recovery strategies can meet the SRTO for critical business services and the RTO for critical business functions.
7.1	Testing	The FI should conduct regular and comprehensive testing to gain assurance that its response and recovery arrangements are robust, and enable them to continue the delivery of critical business services and functions in a timely and reliable manner following a disruption.	Customers should regularly test the response and recovery arrangements for interruption events. The type of tests to be conducted should be selected based on the importance of critical business services and functions. All test activities should be fully documented. Any gaps and weaknesses identified during the tests should be promptly reported and addressed. The rectification status of each test should be tracked and implemented to ensure that the established recovery strategies can meet the service recovery time objectives (SRTO) for critical business services and the recovery time objectives (RTO) for critical business functions.
7.2	Testing	The FI should plan its test activities to meaningfully test all aspects of its BCM framework, and to meet the following test objectives: (a)validate and measure the effectiveness of the BCPs using appropriate metrics, and remediate any gaps or weaknesses that are identified in the recovery process; (b)familiarize personnel, including those of relevant third parties, involved in business continuity and crisis management with their roles and responsibilities. This includes how the alternate sites and recovery arrangements should be operated,; (c)sensitize senior management and staff involved in crisis management to the potential areas of concern that could arise in crisis situations, and practice making decisions under	Customers can leverage the **Cloud Advisor (TSA)** service to assist with planning and executing business continuity tests. This service is a cloud governance platform that integrates multiple ITOM vertical applications and draws on Tencent Cloud's extensive operational expertise. Through risk inspections, fault drills, and other governance measures, Cloud Advisor optimizes cloud infrastructure. It provides fault injection scenarios across IaaS and PaaS layers, as well as industry-specific drill templates covering typical use cases such as cross-availability zone disaster recovery. This helps customers quickly and efficiently reuse proven solutions based on their business needs, improving system availability. **For stress testing**, Tencent Cloud provides **Penetration Testing Service (PTS)**, which simulates real business scenarios with massive user traffic to comprehensively validate system availability and stability. PTS supports multi-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		simulated conditions; (d)stress test BCPs under severe but plausible scenarios to allow the FI; and (e)verify that the SRTOs of its critical business services and RTOs of its critical business functions can be met through the established recovery strategies.	region traffic generation with millions of concurrent requests and offers features such as traffic recording, scenario orchestration, traffic customization, and advanced script configuration. These capabilities enable Customers to quickly define stress test scenarios based on business models, accurately replicate large-scale application access patterns, and identify potential performance issues in advance.
7.3	Testing	The FI should select the types of tests 17 that best meet these objectives, and set out the frequency and scope18 of these tests to be commensurate with the criticality of the business services and functions. The FI should also properly document all its test records. Gaps and weaknesses identified from the FI′ s business continuity testing should be reported to the senior management.	To support regulatory compliance, 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. Disaster recovery drills typically simulate real-world disaster scenarios, including attack-defense exercises and large-scale failures, to thoroughly assess system resilience, response speed, and recovery capability. After each drill, relevant departments prepare a detailed drill report, which is archived along with the drill plan. The report generally includes the drill objectives and scope, execution plan, participants, preparatory work, key processes and timelines, identified issues, corrective measures and implementation plans, and conclusions. For issues identified during drills, Tencent Cloud implements corrective actions based on the improvement measures outlined in the drill summary report and promptly updates corresponding emergency plans. The audit department monitors the implementation of these corrective actions to ensure effectiveness.
7.4	Testing	The FI should establish a formal process to follow up on the remedial actions identified in each test. The effectiveness of the remediation measures undertaken should also be validated at subsequent tests to ensure proper implementation.	
8.2	Audit	The FI should audit its overall BCM framework and the BCM of each of its critical business services at least once every three years. The audit should assess the adequacy and effectiveness of the FI's BCM. The audit	Customer shall conduct regular audits of its overall Business Continuity Management (BCM) framework and the BCM arrangements for each critical business service through qualified independent parties, track remediation of audit findings, and promptly report

No.	Domain	Summary of Controls	Tencent Cloud's Response
		should pay particular attention to higher risk areas identified from the FI's risk assessment, previous audit findings, and relevant incidents.	significant audit findings and audit reports. To support regulatory compliance, Tencent Cloud performs an annual assessment of the completeness, adequacy, and effectiveness of its business continuity management system and revises BCM documentation based on the assessment results. The evaluation report is submitted to relevant senior management for review. Tencent Cloud also engages independent third-party organizations to audit the implementation of its business continuity management practices to ensure compliance with the ISO 22301 Business Continuity Management System standard. For any non-conformities identified during audits, Tencent Cloud promptly analyzes the actual or potential root causes, evaluates the need and priority for corrective and preventive measures, and implements approved actions. The effectiveness of corrective measures is continuously tracked and documented to ensure proper resolution.
8.3	Audit	The BCM audits should be conducted by a qualified party who possesses the requisite BCM knowledge and expertise to perform the audit, and is independent of the unit or function responsible for the BCM of the FI.	
8.4	Audit	The FI should establish processes to track and monitor the implementation of sustainable remedial actions in response to the audit findings. The FI should escalate any significant audit findings on lapses that may have severe impact on the FI′ s BCM to the Board and senior management. The FI should submit the BCM audit reports to MAS upon request.	
9.1	Incident Management	The FI should have robust processes to manage incidents in order to resume critical business services and functions within the stipulated SRTOs/RTOs. Where the delivery of a business service depends on multiple business functions, an overall coordinator should be appointed to coordinate incident management and recovery across affected functions.	Customer shall establish a robust incident management process and appoint an overall coordinator to manage incidents and recovery activities involving multiple business functions. To support regulatory compliance, Tencent Cloud has developed an Information Security Incident Management Standard and established mechanisms and procedures for incident reporting, response, and resolution. These procedures clearly define the roles and responsibilities of each team involved in incident handling. Tencent Cloud uses an internal security operations system to record security incidents. For detected and identified security incidents,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud analyzes and classifies incidents based on factors such as the nature of the incident, data sensitivity, and impact scope, and promptly notify the personnel responsible for follow-up actions. To ensure the effectiveness and timeliness of the incident response process, Tencent Cloud conducts regular emergency drills related to security incident response and provides ongoing technical training to security team members. These training programs ensure that employees understand and comply with the latest security policies and procedures and are familiar with current information security standards and best practices. For security incidents that may affect Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and based on the scope and severity of the incident.
9.2	Crisis Management	The FI′ s senior management is responsible for steering the FI out of a crisis by overseeing its crisis management activities. To aid the senior management in responding to a crisis, the FI should have in place: (a)a crisis management structure, with clearly defined roles, responsibilities, reporting lines, and chain of command; (b)a set of pre-defined triggers and criteria; (c) Formulate relevant plans and procedures; (d)tools and processes to facilitate timely updating and assessment of the latest situation during a crisis;	Customers should establish crisis management framework, plan, and procedures, including communication strategies and channels for internal and external stakeholders. Senior management of the Customer shall oversee all crisis management activities. To support regulatory compliance, Tencent Cloud has developed crisis management procedures that define crisis levels and specify the processes and responsibilities for crisis prevention, analysis and handling, recovery, and post-crisis improvement. Tencent Cloud has also implemented an incident escalation mechanism to clarify communication paths and responsibility allocation during incidents, improving response efficiency and minimizing potential losses caused by unexpected events. For security incidents that may affect external Customers, Tencent Cloud has established incident reporting mechanisms and multiple communication channels to ensure timely

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(e)a list of all internal and external stakeholders to be informed when a critical business service is disrupted, as well as communications plans and requirements for each stakeholder; and (f)communication channels, to effectively communicate with its stakeholders, including alternative channels that can be used when the primary communication channel is unavailable.	notification to affected parties.
9.4	Communications with External Stakeholders	The FI should ensure that communications to its external stakeholders are proactive, transparent, and factual.	Customers should maintain proactive, transparent, and accurate communication with external stakeholders, develop a public communication plan, and designate spokespersons for media and public engagement. In addition, when the Customer identifies an event that may cause severe business disruption or activates its Business Continuity Plan (BCP), the Customer shall notify MAS within one hour of detecting the event. **To assist Customers in fulfilling communication and notification obligations**, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results
9.5	Communications with External Stakeholders	To facilitate timely public communications, the FI should have a communications plan and prepare drawer media statements that cater to different scenarios and hold statements that can be released immediately in the event of a disruption. Where necessary, the FI should also coordinate with peer FIs through the relevant industry associations to achieve consistent messaging to the public in the event of a widespread disruption. The FI should also identify its designated spokesperson(s) who will be responsible for addressing the media and the public.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses.
9.6	Communications with External Stakeholders	The FI should ensure that MAS is notified as soon as possible, but not later than one hour upon the discovery of incidents where business operations will be severely disrupted, or when the BCP is going to be activated in response to an incident. In the notification, the FI should provide information as per the MAS incident reporting template, such as the assessed impact to its customers and the actions that have been taken	**Tencent Cloud also provides multiple channels** for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.

10

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption



On 1 June 2021, the Monetary Authority of Singapore (MAS) issued the Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption. The paper highlights common but critical risks and control measures that Financial Institutions should consider before adopting public cloud services and provides guidance on identifying and managing risks associated with public cloud adoption. The recommendations primarily focus on areas such as shared responsibility for cybersecurity, identity and access management, application security in public cloud environments, data security and encryption key management, immutable workloads and infrastructure-as-code, cybersecurity operations, cloud resilience risk management, outsourcing due diligence for cloud service providers, vendor lock-in and concentration risk management.

This section summarizes the control requirements in the MAS consultation paper that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists Financial Institutions in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
7	Shared Cyber Security Responsibilities	While CSPs are responsible for "Security-of-the-Cloud", FIs would be responsible for "Security-in-the-Cloud". (a) "Security-of-the-Cloud" refers to the security of the public cloud services under the CSPs' responsibility. In an IaaS or PaaS arrangement, these would typically include the security of the underlying hardware, system software and the hypervisor. For SaaS, this would also include the underlying security of the application software. (b) "Security-in-the-Cloud" refers to the security of the cloud workloads under the FIs' responsibility. In an IaaS or PaaS arrangement, these should typically include securing IT systems components such as applications, operating system and orchestration tools. In a SaaS arrangement, it would generally include managing user account privileges and data access rights.	Tencent Cloud adheres to the principles of openness and sharing in cloud computing services, continuously enhancing the security capabilities of its cloud platform and services. Together with customers, we strive to build a more comprehensive and robust security assurance system for cloud-based business and data. As a cloud service provider, Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Recognizing that customers' level of control 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." Tencent Cloud plans and builds its cloud services in accordance with internationally recognized information security and IT governance standards, strictly complying with applicable laws and regulations on privacy protection and data security in the jurisdictions where it operates. Tencent Cloud has obtained multiple internationally recognized security and compliance certifications, providing customers with cloud products and services that have been audited and certified by authoritative third-
8	Shared Cyber Security	FIs should be aware that while CSPs are responsible for	

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Responsibilities	" Security-of-the-Cloud " , in some cases, FIs may have shared responsibilities for managing the controls implemented by the CSPs.	party organizations.
9	Shared Cyber Security Responsibilities	FIs are reminded to ensure that the cyber security responsibilities of all contracting parties are clearly delineated in their outsourcing agreement with CSPs. FIs should be aware of their security responsibilities and undertake adequate measures to secure their workloads in the public cloud.	Customers should clearly define the cybersecurity responsibilities of both parties in the outsourcing agreement signed with the cloud service provider, and fully understand their own security obligations while taking adequate measures. 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. Tencent Cloud actively supports customers' outsourcing-management requirements by providing dedicated personnel to assist and cooperate with audits or assessments initiated by the customer. It also offers a range of security controls and related cloud products/services to ensure the confidentiality and integrity of customer data in the cloud.
10	Identity and Access Management, IAM	FIs should enforce the principle of " least privilege " 6 stringently when granting access to information assets in the public cloud.	Customers should grant access to assets in the public cloud based on the principle of "least privilege," implement multi-factor authentication for privileged users, regularly rotate or promptly revoke cloud authentication credentials, and adopt industry best practices to ensure security when integrating public cloud workloads with on-premises authentication services.
11	Identity and Access Management, IAM	FIs should implement multi-factor authentication (MFA) for privileged employees.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
12	Identity and Access Management, IAM	Credentials used by system/application services for authentication in the public cloud, such as "access keys", should be changed regularly. If the credentials are not used, they should be deleted immediately.	**From the perspective of access control management,** Cloud Access Management (CAM) can help the customer to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides **Bastion Host (BH),** which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. **To support the integration of cloud resource access control with on-premises authentication services**, Tencent Cloud provides the Cloud Access Management (CAM) supports Single Sign-On (SSO) based on SAML 2.0 and OIDC. External users authenticated through an Identity Provider (IdP) can directly access Tencent Cloud resources. For example, Tencent Cloud supports on-premises enterprise IdPs such as Microsoft Active Directory Federation Service (ADFS) and Shibboleth, as well as cloud-based IdPs such as Azure AD, Google Workspace, Okta, and OneLogin. In addition, 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 also implements authorization policies and privilege separation mechanisms, ensuring through granular permission segmentation that employees are granted only the minimum privileges necessary to deliver corresponding services. Furthermore, When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production
13	Identity and Access Management, IAM	FIs that are integrating public cloud workloads with an on-premises authentication service should adopt prevailing best practices in securing such implementations to minimize contagion risk	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			environment where customer data resides through a bastion host with two-factor authentication. For more information on identity authentication and access control, please refer to Section 7.7: "Access Control."
16	Securing Applications in Public Cloud	Where applications are developed for the public cloud environment, FIs are reminded to adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, conduct robust threat modelling, and implement prevailing best practices in software security. Should FIs use a continuous development-operations process (DevOps), security should be embedded throughout the Continuous Integration/Continuous Development (CI/CD) toolchain. FIs should adopt DevSecOps, which is the practice of automating and integrating IT operations, quality assurance and security practices in their software development process.	Customers should adopt an appropriate Secure Development Lifecycle (SDL) process and DevSecOps practices to ensure application development security in public cloud environments. To support customers in R&D management, Tencent Cloud provides **Cloud Native Build (CNB)** developer tools. CNB is based on the Docker ecosystem, abstracting environments, caches, and plugins, and uses declarative syntax to help developers build software more efficiently. CNB offers a complete developer toolchain with capabilities such as code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and custom task sets, effectively enabling end-to-end R&D process support and agile development management from requirements to deployment. Tencent Cloud has established a set of secure development standards for information systems and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the product secure development lifecycle. This approach addresses different stages including requirements, design, development, testing, delivery, and operations, embedding information security and privacy protection principles into every phase to ensure that cloud products receive adequate security controls and assessments throughout their lifecycle. For more information on

No.	Domain	Summary of Controls	Tencent Cloud's Response
			development lifecycle security, please refer to Section 7.3 "IT Project Management and Security-by-Design" and Section 7.4 "System Development Life Cycle and Security-By-Design".
17	Securing Applications in Public Cloud	FIs should recognize that such an architecture could potentially broaden the attack surface of an application in the public cloud, due to the increased deployment of APIs. FIs should ensure that adequate security controls are in place, including, securing the service discovery mechanism, using service mesh for fine-grain access control to APIs and implementing robust authentication for microservices.	Customers should deploy appropriate security controls, implement fine-grained access control and the principle of least privilege to protect APIs, and establish robust identity and access management to authenticate service requests. Tencent Cloud APIs provide interfaces for various Tencent Cloud product resources, enabling customers to quickly operate cloud products through **TencentCloud API**. Tencent Cloud's Cloud API supports HTTPS transmission encryption, interface authentication through multiple SDK signature mechanisms (such as PHP, Python, Java, .NET, Node.js), uses timestamps to limit signature validity and prevent replay attacks, and supports signature encryption. Tencent Cloud integrates API monitoring and management capabilities, allowing customers to configure API status monitoring for their business needs through the console. In addition, Tencent Cloud provides API protection features to effectively mitigate risks of API failure or misuse. Tencent Cloud uses Access Key as the credential for API calls to cloud resources. Customers can regularly audit keys, disable long-inactive keys, and rotate active keys that have been in use for an extended period to reduce the risk of key leakage.
18	Securing Applications in Public Cloud	When securing APIs, FIs should implement fine-grain access control and adopt the principle of least privilege i.e. strictly limit access to services to what is needed only, with the minimum level of privileges needed. FIs should also enforce robust IAM to authenticate service requests. FIs should not rely on implicit trusts when granting access. For microservices, FIs should not assume that API security is sufficiently provided by API gateways or service mesh proxies and should ensure that prevailing best practices in API security, including secure coding practices, are adopted in the implementation of APIs.	
19	Securing Applications in Public Cloud	FIs should ensure that each container includes only the core software components needed by the application to reduce the	Customers may classify and run containers based on the criticality of the service or the sensitivity of the data being processed and should adopt container-specific security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		attack surface. As containers typically share a host operating system, FIs should run containers with a similar risk profile together to minimize risk exposure. FIs should adopt container-specific security solution for preventing, detecting and responding to container-specific threats.	solutions to detect and respond to container-related threats. Customers should also control access to container orchestrators and container images and use only trusted container images. Tencent Cloud Container Registry (TCR) provides customers with secure, dedicated, and high-performance container image hosting and distribution services. It supports global multi-region on-demand synchronization, fast image replication within the same country, and nearby image pulling. To ensure data security and access compliance, TCR offers image security scanning, permission management, public and private network access control, and compatibility with Cloud Access Management (CAM). Customers can configure TCR access control policies to allow only specified public IP addresses and VPC customers to access instances. Each TCR instance has a dedicated storage backend, and container images and Helm charts are encrypted and stored in the customer's Cloud Object Storage (COS) bucket. Customers can also use Tencent Cloud Container Security Service (TCSS) to protect container and image security. TCSS supports container asset management, image security scanning, runtime intrusion detection, and security baseline configuration management, helping customers build a comprehensive container security protection system. TCSS provides full lifecycle protection for containers—from image creation and storage to runtime. In addition, Tencent Cloud computing products strive to provide customers with secure images, including official public images composed of base operating systems and Tencent-provided initialization components, as well as third-party images that have undergone Tencent Cloud's content review and security verification before being published in the marketplace.
20	Securing Applications in Public Cloud	FIs should ensure stringent control over the granting of access to container orchestrators (e.g. Kubernetes), especially the use of the orchestrator administrative account, and the orchestrators ' access to container images. To ensure that only secure container images are used, a container registry could be established to facilitate tracking of container images that have met the Fis' security requirements.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
21	Data Security and Cryptographic Key Management	FIs should implement appropriate data security measures to protect the confidentiality and integrity of sensitive data in the public cloud, taking into consideration data-at-rest, data-in-motion and data-in-use where applicable. a) For data-at-rest i.e. data in cloud storage, FIs may implement additional measures b) For data-in-motion i.e. data that traverses to and from, and within the public cloud, FIs may implement session encryption or data object encryption in addition to the encryption provided at the platform level. c) For data-in-use i.e. data that is being used or processed in the public cloud, FIs may implement	Customers should implement appropriate data security measures to protect the confidentiality and integrity of sensitive data stored in the public cloud, considering data at rest, data in transit, and data in use (where applicable). Customers should also consider adopting an encryption key management strategy, leveraging Hardware Security Modules (HSM) to protect encryption keys, and ensuring the security of encryption keys managed by the cloud service provider. **For data storage protection**, 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 provides full lifecycle management. **Key Management Service (KMS)** uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		confidential computing solutions if available from the CSPs.	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. Tencent Cloud also employs multi-replica redundant storage and erasure coding technology to ensure data integrity and initiate immediate recovery measures upon detecting errors, significantly improving fault tolerance. **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. **For Tencent Cloud's internal use of encryption algorithms and key management**, Tencent Cloud has established security management standards that define requirements for the secure handling of key lifecycle processes, including application, generation, storage, usage, transmission, rotation, and destruction. All key lifecycle operations follow fundamental principles such as dual control,
22	Data Security and Cryptographic Key Management	FIs should consider adopting cryptographic key management strategies that accord them a high level of control and protection over cryptographic keys used for encrypting sensitive data.	
23	Data Security and Cryptographic Key Management	To secure cryptographic keys used for encrypting sensitive data, FI may consider generating, storing and managing the keys in a hardware security module (HSM) and hosting the HSM in an environment that the FI has a higher degree of control over (e.g. FI′ s own on premise IT infrastructure)	
24	Data Security and Cryptographic Key Management	For cryptographic keys managed by CSPs, FIs should ensure that the CSPs′ cryptographic key management policy, standards and procedures are adequate to protect the keys from unauthorized access, usage and disclosure throughout the cryptographic key management life cycle. This includes key generation, distribution, installation, renewal, revocation, recovery and expiry.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			strict handover, proper custody, and timely updates. During key usage, Tencent Cloud enforces separation of duties, strict approval processes, real-name operations, and maintains detailed business key operation logs, which are subject to regular audits. When using cryptographic algorithms during data transmission and storage, Tencent Cloud requires internal teams to comply with international cryptographic management standards or regulations, adopt high-security algorithms such as AES-256, and ensure key lengths meet prescribed requirements.
25	Immutable Workloads	FIs may consider using immutable workloads to ensure the security and stability of workload components especially during software upgrades or security patching. Testing should be performed on immutable workloads images to ensure that an image is secure and stable before implementing it in the production environment.	Customers should consider adopting immutable workloads and ensure that images are tested before being deployed to production environments. To assist customers in meeting regulatory requirements, Tencent Cloud provides the **Tencent Kubernetes Engine (TKE)**, which is based on native Kubernetes and offers a container-centric, highly scalable, high-performance container management service. TKE is fully compatible with native Kubernetes APIs and extends Tencent Cloud features such as cloud disks and load balancing through Kubernetes plugins. It provides a complete set of capabilities for containerized applications, including efficient deployment, resource scheduling, service discovery, and dynamic scaling, addressing environment consistency issues across development, testing, and operations, and improving the convenience of managing large-scale container clusters. For image management, TKE regularly synchronizes official DockerHub images, supports viewing and using DockerHub repositories, and offers customers secure and reliable private image repositories for creating private images. In addition, **Tencent Cloud Container**

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Registry (TCR) provides secure, dedicated, and high-performance container image hosting and distribution services. Each TCR instance has an exclusive storage backend, with container images and Helm Chart data encrypted and stored in the customer's COS bucket. TCR supports fine-grained permission management, public and private network access control, and image security scanning to ensure data security and access compliance. Customers can also use Tencent Cloud Container Security Service (TCSS) to protect container and image security. TCSS supports container asset management, image security scanning, runtime intrusion detection, and security baseline configuration management, helping customers build a comprehensive container security protection system and providing full lifecycle protection for containers—from image creation and storage to runtime.
26	Immutable Workloads	FIs using Infrastructure-as-Code (IaC) to provision or manage public cloud workloads should implement the necessary controls to minimize the risk of misconfiguration, and avoid using both IaC and non-IaC approaches concurrently in order to reduce the complexity of the IT environment. FIs should also ensure that IaC configuration files are protected from unauthorized access and modification.	If customers configure public cloud workloads using Infrastructure as Code (IaC), they should implement necessary controls to reduce configuration errors and protect IaC configuration files. To help customers manage and secure IaC configurations, Tencent Cloud provides Tencent Infrastructure Automation for Terraform. This product is based on the globally popular IaC tool Terraform and its plugin extension system, offering automated capabilities for cloud resource deployment, implementation, and management. It aims to connect Terraform's mature infrastructure automation capabilities with Tencent Cloud's resource services, enabling customers to easily implement DevOps and multi-cloud deployment models. It is fully compatible with Terraform's HCL declarative syntax, allowing infrastructure resources to be described and version-controlled as code, improving automation efficiency for deployment and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			operations. Customers can use Configuration Audit (Config) to centrally audit and govern cloud resources, continuously recording configuration details and changes for various resources across regions under their account. Based on Tencent Cloud best practice rules and compliance templates, Config automatically performs ongoing compliance assessments of resource configurations under enterprise accounts, identifying non-compliant configurations to enable automated monitoring and management of cloud resources. To support customers in meeting regulatory requirements, 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. Tencent Cloud also operates an internal network monitoring system to monitor and alert on these devices and has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. The EDR tools support antivirus and intrusion detection, security baseline and vulnerability scanning, and compliance auditing of command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviours, and Tencent Cloud follows up and handles alerts through its ticketing system. Additionally, all types of program changes—including configuration files and operating systems—must undergo business impact analysis before release, have rollback plans in place, and be approved by responsible personnel. Tencent Cloud's change release

No.	Domain	Summary of Controls	Tencent Cloud's Response
			system enforces that changes can only be executed by authorized personnel, retains change-related logs, and conducts regular log reviews. After release, Tencent Cloud operations team monitors changes in the production environment and records the results.
27	Cyber Security Operations	To maintain holistic cyber situational awareness of information assets, FIs should avoid performing security monitoring of on-premises applications or infrastructure, and public cloud workloads in silo. FIs should feed cyber-related information on public cloud workloads into their respective enterprise-wide IT security monitoring services to facilitate continuous monitoring and analysis of cyber events.	Customers should implement centralized monitoring and analysis for on-premises applications, infrastructure, and public cloud workloads to maintain comprehensive situational awareness of information assets and security events. To monitor and analyze information assets, customers can use **Tencent Cloud's Observability Platform (TCOP)**, which provides real-time monitoring, analysis, and alerting services for cloud products and resources. TCOP collects monitoring metrics reported by Tencent Cloud products and customer-defined configurations and displays them through visual dashboards, helping customers track operational status and performance in real time. Tencent Cloud also offers a one-stop security management platform, **Cloud Security Center (CSC)**, which aggregates threat alerts and logs from Cloud Firewall and Web Application Firewall, and uses Tencent Cloud threat intelligence and proprietary security knowledge bases for automated analysis and investigation, delivering centralized threat detection, investigation, and response capabilities. Tencent Cloud provides the **Threat Intelligence Center (TIX)**, a one-stop intelligence service platform offering three core intelligence capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports intelligence queries, IOC analysis, and attack surface management, enabling customers to efficiently analyze security incidents and comprehensively assess enterprise asset exposure risks, helping

No.	Domain	Summary of Controls	Tencent Cloud's Response
			organizations build an effective, multi-layered security defense system. Tencent **Cloud Log Service (CLS)** and other log-related products allow customers to download, export, or forward cloud logs to local environments or designated third-party systems, including on-premises SIEM/SOC platforms.
28	Cyber Security Operations	FIs should also ensure that their incident response, handling and investigation processes are adapted for public cloud workloads.	Customers should ensure that incident response, handling, and investigation processes apply to public cloud workloads. To support rapid detection and response, Tencent Cloud has established an Information Security Incident Management Standard, defining reporting, response, and handling mechanisms, as well as roles and responsibilities for each team. Tencent Cloud records security incidents in its internal security operations system. For detected incidents, Tencent Cloud analyzes and classifies them based on nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. The Tencent Cloud security team operates a 24/7 security operations framework focused on vulnerability monitoring, intrusion tracing, and attack mitigation, enabling real-time alert response and rapid development of incident containment and emergency response plans. For security incidents that may affect customers, Tencent Cloud will notify them of the handling and analysis results through appropriate channels after internal review, based on the incident's scope and severity.
29	Cloud Resilience Risk Management	FIs should evaluate the track records of the CSP in maintaining the resiliency of its public cloud services to verify that they are commensurate with the Fis' business needs. Such evaluation should be performed prior to	Customers should evaluate the resilience of public cloud services before and during use and consider deploying workloads across multiple geographically dispersed locations. Tencent Cloud data centers span multiple regions worldwide, including Mainland China, Asia-Pacific, North America, and Europe, organized

No.	Domain	Summary of Controls	Tencent Cloud's Response
		engaging the service of a CSP, and on a regular basis after engaging the CSP.	into regions and availability zones. Customers can flexibly deploy data and systems across different regions or zones according to business needs and security requirements, adopting various business continuity models to meet disaster recovery objectives.
30	Cloud Resilience Risk Management	FIs should be aware that their cloud workloads are not resilient by virtue of being in the public cloud. For cloud workloads that require high availability, it is the FI′ s responsibility to ensure that the CSP has appropriate cloud redundancy or fault-tolerant capability and that the appropriate features are enabled for the cloud workloads. Cloud workloads could also be deployed in multiple geographically separated data centres (e.g. "zones" or "regions") to mitigate location-specific issues that may disrupt the delivery of public cloud services.	Tencent Cloud's computing, networking, storage, database, container, middleware, and security services are designed for high availability and include corresponding disaster recovery plans. Tencent Cloud has established a comprehensive Business Continuity Management (BCM) system and obtained ISO/IEC 22301 international certification for BCM. For more details on cloud resilience and business continuity, please refer to Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management." Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon customer requirements, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports.
31	Cloud Resilience Risk Management	FIs should be proactive in monitoring the maintenance schedule, service disruptions, changes to services and end-of-life of services announced by the CSPs, such as via the CSPs′ websites or through the cloud meta structure, so as to be able to take timely measures to ensure that Fis' systems remain available.	Customers should proactively monitor updates released by the cloud service provider regarding cloud services, including maintenance schedules, service interruptions, service changes, and service termination. Tencent Cloud communicates such information promptly through various channels, including official product announcements, console notifications, email, and SMS, to minimize any negative impact these changes may have on customers' system availability.

No.	Domain	Summary of Controls	Tencent Cloud's Response
32	Outsourcing Due Diligence on CSPs	In considering a cloud outsourcing arrangement, FIs should ensure that their ability to manage risk and meet regulatory requirements/expectations is not impeded by contractual terms and conditions.	Customers should ensure that the contractual terms and conditions agreed with the cloud service provider do not restrict their own audit and information access rights or those of relevant regulatory authorities, enabling proper outsourcing due diligence and supervisory review. For customer audits and regulatory reviews, Tencent Cloud will cooperate with third-party security audits and inspections initiated by customers, based on actual circumstances and contractual agreements, and will provide dedicated support personnel to actively assist and respond to audit activities.
33	Outsourcing Due Diligence on CSPs	FIs should ensure that independent audits and/or expert assessments of cloud outsourcing arrangements are conducted as part of their outsourcing due diligence and risk management.	Customers should conduct independent audits and/or expert assessments of cloud outsourcing arrangements. To support customers' outsourcing oversight requirements, Tencent Cloud will, in accordance with actual circumstances and contractual agreements, cooperate with third-party audits and provide dedicated assistance, actively responding to customer-initiated audit activities. Additionally, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture and ensure compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes regular independent third-party professional audits and provides assurance reports on system and organizational controls to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud services. For more information on Tencent Cloud's certifications and completed third-party independent assessments/audits, please refer to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Section 2: "Tencent Cloud Security and Privacy Compliance."
35	Vendor Lock-in and Concentration Risk Management	To mitigate the risks of vendor lock-in, FIs may adopt cloud portability or interoperability solutions, and use open standards for data and software interfaces to facilitate redeployment of cloud workloads to an in-house IT infrastructure or public cloud infrastructure managed by another CSP. For cloud workloads that are critical to the FIs, exit strategies should be developed.	Customers should develop exit strategies for cloud workloads related to critical business and consider adopting cloud portability and interoperability solutions, as well as open-standard interfaces to facilitate workload migration. If customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate cloud data and production environments at any time. According to the service agreement between Tencent Cloud and the customer, if the cloud service expires or is terminated, customers must complete data migration before the retention period ends for any data stored on cloud servers through Tencent Cloud services. Tencent Cloud supports customers in backing up and migrating data using common standard formats. Customers can use the same transmission methods and protocols as during onboarding or leverage network services such as **Direct Connect (DC)** and **VPN Connection** to ensure secure and reliable data transfer during offboarding. After cloud services are terminated, Tencent Cloud will follow strict data erasure procedures and permanently delete all customer data, including replicas and backups, after the retention period. Deleted data cannot be restored.
37	Skillset	FIs should ensure that their cloud risk management strategy considers whether staff have the requisite expertise and experience to understand and manage the risks of public cloud adoption. FIs should ensure staff have the necessary knowledge and skillset to manage the attendant	Customers should ensure that employees possess the necessary knowledge and skills to manage the technologies and network risks associated with cloud services used within their organization. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technology and cyber risks for different cloud services which are used in their organizations.	relevant professional expertise to enhance customers' technical capabilities and cloud proficiency. Tencent Cloud also provides multiple support channels, including 24/7 ticketing, 24/7 hotline, intelligent customer service, and self-service options, to continuously address customer inquiries and feedback. Tencent Cloud's support team and technical experts deliver prompt and effective assistance. To help customers comply with regulatory guidance, Tencent has established a Security Technology Committee and 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.

11 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Control Objectives and Procedures for Outsourced Service Providers

The Association of Banks in Singapore (ABS) has established the "Guidelines on Control Objectives and Procedures for Outsourced Service Providers", which define the minimum baseline control requirements for outsourced service providers (OSPs) serving financial institutions. By adhering to these guidelines, OSPs can assure financial institutions that their control design and operational effectiveness meet the required standards. In addition, OSPs must provide an OSPAR audit report issued by an independent third party. The requirements primarily cover areas such as audit and inspection, entity-level controls, general IT controls, and service-level controls.

In this section, Tencent Cloud summarizes the control requirements in the OSPCOP Guidelines that are relevant to cloud service providers and explains how Tencent Cloud, as a CSP, complies with these requirements.

11.1 Audit and Inspection of Technology Risk Governance and Oversight

No.	Domain	Summary of Controls	Tencent Cloud's Response
I	Engagement of External Auditor	The OSP should engage a qualified auditor to perform audits in accordance with these Guidelines on the services rendered to the FIs. In the event that an OSP decides to change the external auditor or decides to appoint a different external auditor for validation of remediation activities (refer to section "V. REPORTING AND HANDLING OF CONTROL FAILURE / QUALIFICATION OF CONTROL OBJECTIVES"), the OSP must ensure that there is a proper hand-over from the outgoing auditor to the incoming auditor to ensure that the interests of the FIs remain protected.	Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments. Based on customer needs, Tencent Cloud also provides assurance reports on system and organizational controls to disclose the latest internal control status of its service organization to cloud customers, independent auditors, regulators, shareholders, and other stakeholders. Specifically for Singapore, to ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Singapore's financial regulations, Tencent Cloud engages an independent third-party audit firm annually to audit its internal control framework and issue the Outsourced Service Provider Audit Report (OSPAR) under the Association of Banks in Singapore. Customers can download the latest OSPAR report directly from **Tencent Cloud's Compliance Documentation Center**.
II	Criteria for Qualification External Auditor	The appointed external auditor should demonstrate a sound understanding of outsourcing risks pertinent to the FI industry as well as fulfil the following criteria:	When selecting audit firms, Tencent Cloud follows the requirements outlined in this guide to ensure that the chosen firm has extensive project experience in Singapore's

No.	Domain	Summary of Controls	Tencent Cloud's Response
		1. The audit firm must have audited at least 2 commercial banks operating in Singapore in the last 5 years; and 2. The engagement partner, who signs off the Audit Report, must have audited at least 2 commercial banks operating in Singapore in the last 5 years.	financial industry. Tencent Cloud also stipulates in its agreements with audit firms that, in the event of a change of audit firm or auditor during the process, the outgoing auditor must properly hand over to the incoming auditor.
III	Frequency of Audit	The audit should be performed once every 12 months. The samples selected for testing the operating effectiveness of controls should cover the entire period since the previous audit, with a minimum testing period of 6 months. If the period is less than 6 months, the reasons for the shorter period should be provided in the report.	
IV	Audit Reort	The appointed external auditor should issue the audit report in the format stated in the Outsourced Service Provider Audit Report ("OSPAR") template. The OSP must furnish a copy of its audit report to its FI customers.	
V	Reporting and handling of control Failure/Qualification of Control Objectives	Where the auditor identifies a failure in the design and/or operating effectiveness of a control activity in relation to a control objective, the auditor should assess the potential impact of the failure on the services provided to the FIs. The auditor should be guided by the relevant auditing	During the audit process, Tencent Cloud will provide evidence of the design and/or operating effectiveness of control activities related to control objectives, as required by the auditing body. For any issues identified during the audit, Tencent Cloud will conduct a root cause analysis and develop and implement appropriate remediation measures and corrective action plans. If such issues may affect the business operations or

No.	Domain	Summary of Controls	Tencent Cloud's Response
		standards which specify the procedures for qualification of a control objective. OSPs should notify the FIs of significant issues and concerns, and the remediation plans no later than the OSPAR release date. However, OSPs should notify the FIs immediately if the issues could potentially lead to a prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the FI ' s customer information. The OSP should develop remediation plans to address the issues identified by the audit. If the issues require an extended time period to correct, the OSP should identify short term measures to mitigate the risks. The remediation measures should be validated by the auditor or other competent independent party.	data security of financial institution customers, Tencent Cloud will promptly notify the relevant institutions. Tencent Cloud will regularly follow up on the execution of remediation measures and corrective plans until the audit findings are closed.
VI	Rights of Fis and MAS	The MAS and FIs retain the right to audit the OSP, as well as the OSP' s sub-contractors.	Tencent Cloud will, as appropriate, assign dedicated personnel to actively respond to and support audit and supervisory requirements from customers and the Monetary Authority of Singapore (MAS) regarding Tencent Cloud and its subcontractors.

11.2 Physical Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
I.(a)	Control Environment	The control environment sets priority and culture for the OSP, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure.	Tencent Cloud's control environment follows a top-down management approach, with senior management playing a key role in setting the company's tone and core values. To foster a fair and positive culture across the organization, Tencent Cloud has established a Code of Conduct that defines expected employee behavior. Disciplinary actions are based on principles of timeliness, fairness, impartiality, and transparency.
I.(b)	Risk Assessment	The OSP should establish a risk management framework to manage enterprise risks, technology risks, etc. Appropriate governance structures and processes are established, with well-defined roles, responsibilities, and clear reporting lines across the various organizational functions.	Tencent Cloud has implemented a comprehensive risk management framework in accordance with ISO/IEC 27001:2022 and conducts at least one information security risk assessment annually. The risk assessment process includes the following stages: • Identification: Identifying risks (threats and vulnerabilities) within the environment to provide the foundation for all risk management activities. • Assessment: Evaluating the potential impact and likelihood of identified risks on business processes, as well as the effectiveness of internal controls. • Mitigation: Implementing controls, physical security measures, and virtual security measures to detect and prevent identified and assessed risks. • Reporting: Providing risk assessment reports to management, including data required for informed business decisions and compliance with internal policies and applicable regulations. • Review: Verifying that corrective measures have been implemented and are operating effectively.

No.	Domain	Summary of Controls	Tencent Cloud's Response
I.(c)	Information and Communication	Adequate information and effective communication are essential to the proper functioning of internal control. Communication to the OSP's internal and external stakeholders for any matters related to ordinary course of business or business disruption/crisis should be done in a timely manner.	**Tencent Cloud offers multiple internal communication channels** to help employees understand their roles and responsibilities: • Job descriptions are defined for each position, and employee details such as role, department, and reporting structure are maintained on internal platforms. • Security violations and corresponding disciplinary actions are published internally. • Internal policies and standards are regularly updated in compliance with laws and regulations, and employees can access them via internal platforms. • A series of training programs, including security awareness and skills development, are provided. • Employee performance evaluations are conducted every six months. **Tencent Cloud also maintains various external communication channels with customers:** • Console ticketing services and online consultations to collect feedback and respond to inquiries regarding security, availability, and confidentiality. • Notifications via console announcements, SMS, and email to communicate potential issues and impacts. Tencent Cloud offers online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, which clearly define the scope and level of services provided, including confidentiality and disclosure responsibilities of both parties.
I.(d)	Monitoring	The OSP may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, either by	Tencent Cloud has established internal audit management procedures to standardize the planning and execution of internal audits. Nonconformities identified during audits are

No.	Domain	Summary of Controls	Tencent Cloud's Response
		ongoing activities, periodic evaluations, or combinations of the two. OSPs should have processes in place to bring significant issues and concerns identified through such evaluation to the OSPs ′ senior management and additionally, if impacting the services provided, e.g. adverse developments, to the FIs. The OSP′ s monitoring of its sub-contractors ′ activities that affect the services provided to the FIs is another example of monitoring.	documented in audit reports and approved by management. Responsible departments must develop and implement corrective actions, which are tracked by the internal audit team. Tencent Cloud has obtained multiple security and privacy compliance certifications through independent third-party audits or assessments. It provides assurance reports on system and organizational controls to disclose the latest internal control status to cloud customers, independent auditors, regulators, shareholders, and other stakeholders. To meet Singapore financial regulatory requirements, Tencent Cloud engages an independent audit firm annually to review its internal control framework and issue the Outsourced Service Provider Audit Report (OSPAR) under the Association of Banks in Singapore. For audit findings or nonconformities that may affect customers, Tencent Cloud will notify customers of the analysis and remediation plan through appropriate channels after internal review. Tencent Cloud continuously monitors subcontractor service levels to ensure secure and stable operations. It evaluates subcontractor performance against contractual security and operational standards and takes corrective actions when necessary to maintain compliance with established security and quality requirements.
I.(e)	Information Security Policies	Information Security ("IS") policies and procedures are established, documented and reviewed at least every 12 months or as and when there are changes. IS policies and procedures should state the person(s) responsible for information security management.	Tencent Cloud has established an Information Security Management Policy comprising an overall security strategy, organizational structure, and management system to support secure cloud platform operations and risk management. The policy is reviewed annually to ensure that control objectives, procedures, and measures comply with relevant security strategies, standards, procedures, and legal requirements. Employees can access these

No.	Domain	Summary of Controls	Tencent Cloud's Response
		An information security awareness training programme should be established.	policies via internal platforms. Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements. Tencent Cloud integrates information security management into daily operations to ensure employees understand and comply with internal policies and requirements.
I.(f)	Human Resource Policies and Procedures	The OSP should establish standards for workplace conduct, implement candidate background screening procedures, and conduct enforcement procedures to enable it to meet its commitments and requirements as they relate to the ABS controls objectives and Requirements for the management of outsourced Services by the MAS.	Tencent Cloud has established robust HR management standards and procedures to ensure appropriate recruitment and placement based on job requirements. Background checks, including verification of education and certifications, are conducted during recruitment. Upon employment, internal staff and external third parties must sign confidentiality agreements outlining obligations and requirements. Confidentiality clauses are periodically reviewed and updated by the legal department to ensure applicability and compliance. Tencent Cloud has also developed a Code of Conduct that defines prohibited behaviors and corresponding disciplinary measures for violations of information security requirements.
I.(g)	Practices related to Sub-Contracting / Third Parties related to Delivery of Service	OSP should require and ensure that their sub-contractors/ third parties adhere to the requirements of these Guidelines. The OSP ' s monitoring of its sub-contractors ' activities that affect the services provided to the Fis.	Tencent Cloud signs formal contracts with subcontractors to ensure compliance with this guide, clearly defining security, privacy, and confidentiality responsibilities and obligations. Tencent Cloud continuously monitors subcontractor service levels and evaluates performance against contractual security and operational standards, taking corrective actions when necessary to ensure compliance with established security and quality requirements.

11.3 General Information Technology Controls

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.(a)	Logical Security	Logical access to programmes, data, and operating system software is restricted to authorized personnel on a need-to-have basis.	**In terms of user authorization**, 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. Regular internal permission reviews are conducted to prevent misuse or abuse of access rights. Any unnecessary access rights are promptly revoked. **For privileged account management**, Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before accessing bastion hosts, and authorized personnel must complete secondary identity verification to log in. All backend operation records are stored centrally on a logging platform and reviewed periodically by Tencent Cloud's internal audit team. **For remote access management**, Tencent Cloud employees may only use trusted devices registered with Tencent Cloud and must access Tencent Cloud's office network and daily systems through encrypted communication channels. Remote access logs are maintained and reviewed regularly. **Regarding customer account registration and usage**, customers must read and accept the Tencent Cloud Service Agreement during account

No.	Domain	Summary of Controls	Tencent Cloud's Response
			registration on the official website. This agreement defines responsibilities and obligations related to access management. The management console serves as the central control point for managing and controlling cloud resources. When customers register a cloud account, the console automatically checks for account name uniqueness. Authentication information is transmitted via HTTPS when customers log in to the console. Customers can centrally manage cloud services and data through open APIs. When registering for Open API functionality, customers must use the access keys assigned to them for authentication. Before accessing cloud services, customer identity is verified using these access keys. Customers can enable multi-factor authentication to enhance security for account logins and sensitive operations such as password changes. **To protect encryption keys used for securing sensitive data**, Tencent Cloud has established encryption and key management standards governing key application, generation, storage, usage, transmission, rotation, and destruction. All key lifecycle operations follow strict requirements for dual control, secure handover, proper storage, and timely updates. Key usage must comply with principles of segregation of duties, strict approval, and real-name operations, with key operation logs retained for periodic audits. Business teams are required to manage the entire key lifecycle based on factors such as key purpose, data sensitivity, and potential impact of key compromise.
II.(b)	Physical Security	Data Centre/Controlled Areas are physically secured from internal and external threats.	**For physical environment security**, Tencent Cloud has implemented physical security management policies to standardize operational safety, promptly identify risks, and strengthen physical security controls. Tencent Cloud's global data centers are selected, built, or leased in compliance with relevant international standards and local security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			requirements. In Singapore, Tencent Cloud operates four leased data centers. To ensure resilience and security, Tencent Cloud has established a rigorous management system covering supplier onboarding, contractual obligations, and continuous oversight. Annual internal and external audits include on-site inspections of operator data centers to verify compliance with Tencent Cloud's information security requirements. Tencent Cloud requires operators to equip data centers with complete fire protection systems and highly stable, fully redundant power and cooling systems to prevent single points of failure from impacting continuity. **For physical access control**, Tencent Cloud requires operators to implement formal access procedures, verify personnel identity, and inspect and register carried items. Operators must regularly review access permissions to ensure proper allocation and timely revocation of unnecessary rights. For external visitors, operators must establish visitor application and authorization mechanisms, allowing only approved visitors to access designated areas at scheduled times under staff escort. Operators must also implement approval and inspection processes for equipment entering or leaving server rooms (e.g., installation, decommissioning, or relocation). **For security and monitoring**, Tencent Cloud requires operators to conduct daily inspections of server rooms and equipment according to predefined checklists and schedules, recording signatures and timestamps at each checkpoint. Operators must immediately activate emergency response procedures upon detecting infrastructure failures or security incidents. Data centers must be equipped with 24/7 video surveillance systems with no blind spots, monitored from a security control room, and ensure secure retention of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			surveillance records for an adequate duration.
II.(c)	Change Management	Changes to applications, systems software and network components are assessed, approved, tested, implemented and reviewed in a controlled manner.	Tencent Cloud has established product and configuration change management standards defining all steps and responsible parties in the change process to ensure proper approval and testing before implementation. Emergency changes follow a dedicated management process and require appropriate approval prior to execution. All program changes—including application, configuration files, operating systems, and databases, must undergo business impact analysis, have rollback plans in place, and be approved by responsible personnel before deployment. Tencent Cloud's change release system enforces that only authorized personnel can execute changes, retain change-related logs, and conduct regular log reviews. After release, requesters must perform post-deployment acceptance testing, and Tencent Cloud operations team monitors changes in the production environment and records results. For more details, refer to Section 7.5 "IT Service Management."
II.(d)	Incident Management	All system and network processing issues are resolved in a timely and controlled manner.	**For incident detection and response**, Tencent Cloud has established a detailed incident management process and uses an internal security operations system to record security incidents. Detected incidents are analysed and classified based on nature, data sensitivity, and impact scope, and relevant personnel are promptly notified for follow-up. Tencent Cloud's security team operates a 24/7 security operations framework focused on vulnerability monitoring, intrusion tracing, and attack mitigation, enabling real-time alert response and rapid development of containment and remediation plans to prevent incident escalation. **For incident notification**, Tencent Cloud communicates the analysis and resolution of security incidents that may affect customers through appropriate channels after internal review.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers can report issues to Tencent Cloud via the console ticketing system, which supports reporting of faults, incidents, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priorities through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of customer needs. **For incident review and continuous improvement**, Tencent Cloud conducts periodic incident analysis, performing multidimensional reviews (e.g., type, frequency, impact scope, severity) and implementing preventive measures based on root cause analysis to avoid recurrence. For major security incidents, Tencent Cloud forms dedicated task forces to produce detailed analysis reports for management. For more details, refer to Section 7.5 "IT Service Management."
II.(e)	Backup and Disaster Recovery	Ensure information systems recovery plans are documented, approved, tested and maintained. Backups are performed and securely stored.	**For recovery planning**, Tencent Cloud develops tailored disaster recovery strategies and business continuity plans based on business impact analysis for cloud products and services. Detailed recovery plans are regularly tested to ensure feasibility. Tencent Cloud has implemented a comprehensive business continuity and disaster recovery management system certified to ISO/IEC 22301. To ensure service availability, Tencent Cloud operates or leases data centers worldwide in compliance with international standards and local security requirements, offering multi-region and multi-availability zone options to meet disaster recovery and service level requirements. Tencent Cloud's compute, network, storage, database, container, middleware, and security services feature high availability and corresponding disaster recovery plans. For more details, refer to Section 7.6 "IT Resilience" and Section 9: "How Tencent Cloud Meets and Assists Customers to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Meet the Requirements of Guidelines on Business Continuity Management". **For backup management**, Tencent Cloud has established internal backup management policies and processes. Product teams must define and implement backup strategies based on business needs and data sensitivity, including backup frequency, method, and retention period. Regular backup restoration tests are conducted to verify data integrity and recoverability, ensuring secure and reliable backup storage. Tencent Cloud also provides customers with options to configure their own backup strategies for systems and data. For more details, refer to Section 7.6 "IT Resilience," **Clause 8.4 "System Backup and Recovery".**
II.(f)	Network and Security Management	Systems and network controls are implemented based on Fis' business needs.	**For system and network security baselines**, Tencent Cloud has established configuration and baseline standards to standardize security settings for network devices, firewalls, servers, operating systems, databases, and applications. Continuous scanning tools detect deviations from standards in operating systems, database management systems, and virtual images. Identified deviations automatically generate security tickets for timely remediation. Tencent Cloud also review network device policies and parameters regularly to ensure effectiveness. **For endpoint security**, Tencent Cloud deploys Endpoint Detection and Response (EDR) tools to monitor and manage all server endpoints. EDR capabilities include antivirus and intrusion detection, baseline and vulnerability scanning, and compliance auditing of command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviors. For employee office Terminal (including laptops and workstations), Tencent Cloud uses a Zero Trust security management system to enforce security controls, including malware removal, vulnerability patching, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			proactive defense, providing comprehensive protection against ransomware, phishing, and lateral movement attacks. The system also supports sensitive data exfiltration monitoring, auditing, and blocking of file transfers via email, cloud storage, remote control, and other channels to prevent data theft. **For patch management**, Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Tencent Cloud also operates internal vulnerability scanning and external vulnerability reporting platforms to track and remediate issues. Security tickets are logged in the operations system and assigned to responsible teams for timely resolution. Tencent Cloud's security research team integrates virtual patching capabilities into its Web Application Firewall to enhance overall platform security. **For network security controls**, Tencent Cloud deploys a mature security architecture with multiple layers of defence, including firewalls, IDS/IPS, DDoS protection, network segmentation, and web application security. Internal network monitoring systems provide real-time alerts, and automated auditing tools detect abnormal behaviours and trigger alerts. Tencent Cloud maintains detailed emergency response plans for various scenarios, including cyberattacks, data breaches, equipment failures, and disasters, and regularly reviews and tests these plans to ensure effectiveness. **For network security event monitoring**, Tencent Cloud has implemented an internal network monitoring system to track and alert on network device status, with identified security issues followed up and resolved through a ticketing system. In addition, Tencent Cloud has established detailed operational security "red

No.	Domain	Summary of Controls	Tencent Cloud's Response
			lines" and, leveraging years of experience in abnormal behavior monitoring, developed a comprehensive rule base and a reliable automated auditing tool for operational security. This enables timely detection of abnormal behaviours and automatic alert triggering.
II.(g)	Security Incident Response	Appropriate personnel within the OSP are contacted and immediate action is taken in response to a security incident.	Based on different network security emergency scenarios—such as cyberattacks, data breaches, equipment failures, and disasters—Tencent Cloud has developed contingency plans and response procedures to ensure orderly and timely handling of security incidents, minimizing negative impacts on Tencent Cloud. These emergency plans are regularly reviewed, updated, and tested to ensure effectiveness. **For incident communication and notification**, Tencent Cloud has established an Information Security Incident Management Policy, including procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal personnel, customers, and other affected parties, enabling efficient and coordinated communication. **For security incidents that may impact customers**, Tencent Cloud communicates the analysis and resolution results through appropriate channels after internal review and provides technical support to help customers take remedial measures and minimize losses.
II.(h)	System Vulnerability Assessments	Ensure vulnerability assessments and penetration testing are conducted regularly to detect and remediate security vulnerabilities in the IT environment.	Tencent Cloud has implemented regular vulnerability scanning and penetration testing mechanisms. Automated scanning tasks are scheduled to identify vulnerabilities in cloud assets, followed by analysis, classification, and remediation. The security team conducts large-scale end-to-end penetration tests periodically and targeted tests before major releases or significant changes. Results are communicated via security tickets to responsible departments for timely patching or compensating controls, ensuring that exploitable vulnerabilities are

No.	Domain	Summary of Controls	Tencent Cloud's Response
			properly addressed. Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.
II.(i)	Technology Refresh Management	Ensure software and hardware components used in the production and disaster recovery environment are refreshed timely.	Tencent Cloud has established information asset management standards and lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems. Servers are regularly retired or replaced, and software components (such as operating systems and database systems) are upgraded before end-of-support. Retired hard drives undergo secure physical destruction, with destruction records maintained to ensure complete disposal.
II.(j)	Data Security	Ensure comprehensive data loss prevention policies and measures have been adopted to detect and prevent unauthorized access, modification, copying or transmission of the FI′ s confidential data.	Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access any customer data unless it is necessary for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations, such as investigations by government authorities into criminal activities. Tencent Cloud enforces end-to-end identity verification and maintenance process for data access permissions to ensure the integrity of data assets and the reliability of business services. A real-time monitoring and interception mechanism is in place to detect and prevent any abnormal data access behaviour. For more information on Tencent Cloud data

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security, please refer to Section 7.9 "Data and Infrastructure Security," **Clause 11.1 "Data Security"**.
II.(k)	Cryptography	Ensure industry-accepted cryptographic controls have been implemented to protect data confidentiality, maintain data integrity and authenticity.	**In terms of data storage protection,** multiple Tencent Cloud storage and database products support data encryption using secure, high-strength encryption algorithms. Integrated Key Management Service (KMS) ensures full lifecycle management of encryption keys, safeguarding data confidentiality. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations. Regarding internal encryption key management, Tencent Cloud has established encryption and key management standards that govern the processes of key application, generation, storage, usage, transmission, rotation, and destruction to ensure the confidentiality, integrity, and availability of keys. For more details on key management, please refer to Section 7.8 "Cryptography," **Clause 10.2 "Key Management"**.
II.(l)	Software Application Development and Management	Ensure policies and measures relating to secure coding, source code review and application security testing have been implemented.	**In terms of secure development processes**, Tencent Cloud integrates its software development lifecycle into DevSecOps practices to ensure rapid and continuous development, release, and deployment of cloud products. Internally, Tencent Cloud has established a set of secure development standards for information systems and incorporates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the secure development lifecycle. This approach addresses all stages—requirements, design, development, testing, delivery, and operations—embedding

No.	Domain	Summary of Controls	Tencent Cloud's Response
			information security and privacy protection principles into every phase to ensure adequate security controls and assessments across the product lifecycle. Tencent Cloud computing products also strive to provide customers with secure images, including official public images composed of base operating systems and Tencent-provided initialization components, as well as third-party images that undergo Tencent Cloud's content review and security validation before being published in the marketplace. **For secure coding and code review**, Tencent Cloud has established detailed secure coding guidelines that internal developers must strictly follow. Tencent Cloud provides secure programming training to enhance developers' awareness of risks such as injection attacks and sensitive data leaks. During development, developers are required to consider security features within application systems to minimize vulnerabilities. Tencent Cloud's internal code security analysis framework integrates capabilities such as Static Application Security Testing (SAST), open-source component scanning, and sensitive information detection. Business teams can leverage pipeline-based self-service scanning during the code admission phase to perform security assessments. Typical issues identified during code reviews are documented and consolidated into the team's knowledge base. **For application security scanning**, Tencent Cloud requires business teams to connect web application test environments to web vulnerability scanning tools for automated scanning before product launch. If vulnerabilities are detected, tickets are automatically generated and assigned to the development team responsible for remediation prior to release, ensuring security issues are not carried into production. **For third-party product usage**, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defense before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies. **Regarding API security**, as the cornerstone of Tencent Cloud's open ecosystem, Cloud APIs cover services provided externally and are continuously iterated. Tencent Cloud APIs supports HTTPS transmission encryption, interface authentication through multiple SDK signature mechanisms, and use timestamps to limit signature validity and prevent replay attacks. In addition to HmacSHA1, Tencent Cloud supports the more secure HmacSHA256 for signature encryption, ensuring the security and integrity of API requests and providing port-level communication security for customer business operations. Tencent Cloud has established internal API security standards and integration guidelines, requiring API risks to be considered during product security assessments. Product APIs must integrate with the Cloud API 3.0 gateway and implement access control for authentication. Sensitive operations and data query interfaces must include access control measures such as rate limiting, query limits, IP whitelisting, and time-based access restrictions. For more information on secure software development lifecycle processes, secure coding, source code review, application testing, and API security management, please refer to Section 7.4 "Software Development Life Cycle and Security-By-Design".

11.4 Service Level Controls

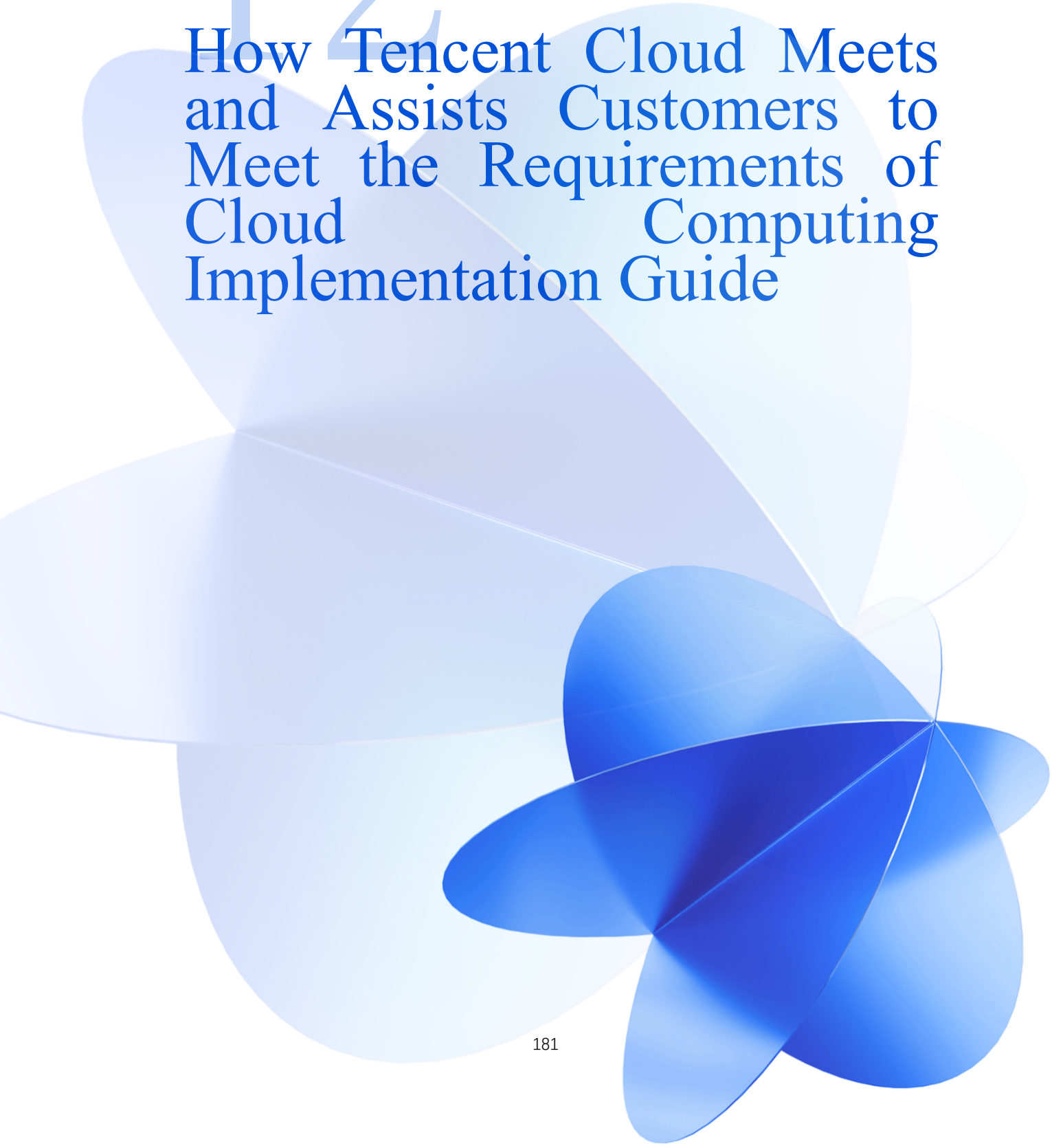
No.	Domain	Summary of Controls	Tencent Cloud's Response
III.(a)	(a) Setting up of New Customers/ Processes	Ensure client contracting procedures are defined and monitored, and client processes are set up and administered in accordance with client agreements/instructions.	Tencent Cloud will cooperate with customers' third-party security audits and inspections based on actual circumstances and contractual agreements, providing dedicated support personnel to actively assist and respond to customer-initiated audit activities. For more details on due diligence, please refer to Section 8: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Outsourcing (Banks) and the Guidelines on Outsourcing (Financial Institutions (Non-Bank Financial Institutions)," **Clause 3.3.2/5.4.2 "Evaluation of Service Providers."** On its international portal, Tencent Cloud provides online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions.
III.(c)	Maintaining Records	Ensure the OSP classifies data according to sensitivity, which determines protection requirements, access rights and restrictions, and retention and destruction requirements.	Tencent Cloud has established processes and requirements for data collection, classification, retention, and destruction to ensure secure data management throughout its lifecycle. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees do not attempt to access any customer data unless required for service delivery and explicitly authorized by the customer. Tencent Cloud strictly adheres to the principle of "data confidentiality," employing multi-layered technical isolation measures to ensure that customer data within the same resource pool remains invisible to other tenants, preventing

No.	Domain	Summary of Controls	Tencent Cloud's Response
			unauthorized access, retrieval, or tampering. If customers need to terminate or exit cloud services, they may back up and migrate cloud data and production environments at any time. Tencent Cloud supports data backup and migration using standard formats, allowing customers to use the same transmission methods and protocols as during onboarding or leverage network services such as **Direct Connect (DC)** and **VPN Connection** to ensure secure and reliable data transfer during offboarding. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data—including replicas and backups—after the retention period. Deleted data cannot be restored. When media used to provide Tencent Cloud services fails or reaches end-of-life, Tencent Cloud performs secure physical destruction following strict procedures.
III.(d)	Safeguarding Assets	Ensure physical assets held by the OSP are safeguarded from loss, misappropriation and unauthorized access.	Physical access to Tencent Cloud office areas is controlled through multiple security measures, including security personnel, access card systems, and CCTV monitoring. Visitors must register with security and deposit all electronic devices prior to entry, and the carrying of any portable storage devices into the data center is strictly prohibited. All visitors must be accompanied by an authorized employee at all times while in the controlled areas of the data center.. All activities within office areas are monitored via 24/7 CCTV surveillance. Tencent Cloud requires data center operators to implement formal physical access procedures to control personnel and equipment entry and exit. For more details on data center access controls, refer to Section 11.3 "General Information Technology Controls," **Clause II(b) "Physical Security."** For information asset management, physical assets are assigned to designated custodians and registered in Tencent Cloud's internal asset

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management system. Annual inventory checks confirm asset existence and record results.
III.(e)	Service Reporting and Monitoring	Ensure the OSP' s engagement with FIs and sub-contractors handling material outsourcing and Fis' customer information are properly managed.	Tencent Cloud delivers cloud services based on agreed Service Level Agreements (SLAs). Performance metrics, measurement standards, and reporting requirements are clearly defined in each SLA and published on Tencent Cloud's official website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console. Tencent Cloud enforces strict supplier security assessments, periodic monitoring, annual evaluations, independent audits, and formal outsourcing agreements to ensure effective supplier management. If Tencent Cloud subcontracts any business, customers are promptly notified, and subcontracting terms are defined in the agreement.
III.(f)	Business Continuity Management	Ensure business continuity plans are documented, approved, tested and maintained.	Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, achieving ISO/IEC 22301 certification for its BCM system. To ensure service availability, Tencent Cloud regularly conducts business impact analyses for cloud products and services, defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and develops contingency strategies and continuity plans based on analysis results. Regular drills are conducted to validate plan effectiveness. Based on customer needs, Tencent Cloud actively participates in disaster recovery exercises involving managed information assets. For more details on business continuity, refer to Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management."

12

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Cloud Computing Implementation Guide



The Association of Banks in Singapore (ABS) launched the Cloud Computing Implementation Guide 3.0 in July 2024 as an industry best practice. The guide aims to help financial institutions manage risks related to cloud third-party security and support the secure adoption of cloud services. Its provisions primarily focus on the minimum recommended due diligence activities prior to entering into cloud third-party agreements, as well as the minimum recommended controls when establishing such arrangements.

In this section, Tencent Cloud summarizes the control requirements in the Cloud Computing Implementation Guide that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in meeting these requirements.

12.1 Cloud Risk Assessment & Due Diligence

Section 2, Part 2 of the Cloud Computing Implementation Guide — "Cloud Third-Party Due Diligence"—sets out the minimum recommended due diligence activities prior to entering into cloud third-party agreements. It requires financial institutions to ensure that their existing risk management framework and third-party due diligence processes can address risks associated with the use of cloud services, cloud service providers, and their significant subcontracting arrangements.

When requested by customers, Tencent Cloud actively cooperates by providing the necessary information to facilitate their due diligence process. The following describes Tencent Cloud's compliance with each due diligence assessment dimension as a cloud service provider.

No.	Domain	Summary of Controls
Pre and Post Implementation Reviews	FIs should establish their own third-party risk management framework and the necessary policies and procedures that are commensurate with the materiality of the arrangement for the scope of their pre- and post-implementation reviews.	To comply with customers' outsourcing oversight requirements, Tencent Cloud will cooperate with third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support customer-initiated audit activities. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual independent professional audits by domestic and international third parties. Through System and Organization Controls (SOC) reports, Tencent Cloud provides assurance to cloud customers, independent auditors, regulators, shareholders, and other stakeholders regarding its latest

No.	Domain	Summary of Controls
		internal control status.
Contractual Agreement	When negotiating a contract with a CSP, the FI should ensure that it can contractually enforce agreed and measurable information security and operational requirements.	On its international portal, Tencent Cloud provides online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. For more details on how Tencent Cloud complies with the MAS Outsourcing Guidelines, please refer to Section 5: How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Notice 658: Management of Outsourced Relevant Ser-vices for Banks and Notice 1121: Management of Out-sourced Relevant Services for Merchant Banks."
Service Level Agreements	Enforceable and measurable Service Level Agreements (SLAs) should be negotiated where possible, particularly for material outsourcing arrangements.	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.
Key Indicators ("KIs")	Appropriate KIs (including Key Performance Indicators, Key Risk Indicators, Key Control Indicators), key activities, inputs and outputs should be defined in the SLA.	
Asset Classification	The FI should have a clear policy on the classification of the assets that are outsourced to CSP. Such policy should include the FI's ability to assess and determine the controls necessary for protecting the data confidentiality and	Tencent Cloud's infrastructure span's multiple global locations, organized by regions and availability zones. Each region is an independent geographic area, and each availability zone is an independent fault isolation domain with physical separation. Customers can flexibly deploy data and systems across different regions or zones based on business needs and data security

No.	Domain	Summary of Controls
	integrity and the location where the data should be hosted.	requirements to meet disaster recovery objectives. Tencent Cloud operates four data centers in Singapore, offering a wide range of cloud services including cloud servers, cloud databases, and CDN. Singapore customers can choose to store and process their data locally within Singapore. Tencent Cloud adheres to principles of transparency. Upon request, Tencent Cloud will promptly provide information through appropriate channels regarding data storage locations, cold backup status, and backup storage locations.
Data Confidentiality and Control Ownership	The FI should ensure that the third-party service agreement includes the following requirements: a. Ensure the CSP can protect the confidentiality and integrity of FI′ s information, documents, records and assets. b. If the service agreement with the CSP terminates on expiry or prematurely, the FI has the contractual right to promptly render data inaccessible at the CSP′ s systems. c. Provision to address specific regulatory requirements, such as the right to audit by the MAS and prompt notification of security incidents or technology outages that have a material impact, must also be included in the outsourcing agreement if relevant.	On its international portal, Tencent Cloud provides online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions.
Data Retention	FI must be able to stipulate access to all its data including those used for daily operational purposes and for contingency, disaster recovery or backups. For encrypted data, FI should ensure that the appropriate cryptographic key management is	**For data access and protection aspects**, customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. Tencent Cloud has established strict access control policies and implemented permission management and authorization mechanisms. Bastion hosts are fully deployed in the production environment

No.	Domain	Summary of Controls
	in place and validate the CSP′ s ability to restore the service from backups effectively. Upon exiting a contract with a CSP, FI should ensure that the CSP covers the design and process for data deletion in the scope of an independent audit	to centrally manage administrator account permissions and activities for backend system components. **For data backup and storage security aspects**, Tencent Cloud has implemented backup management procedures in compliance with relevant legal requirements to back up critical data. Internal information is backed up based on data classification, and recovery tests are conducted regularly. For customer cloud data, Tencent Cloud provides multi-replica storage and backup services according to product SLAs and assumes responsibility for backup services as agreed. To ensure confidentiality and integrity, Tencent Cloud storage and database products support encryption using strong algorithms and integrate with the Key Management Service (KMS) for full lifecycle key management. Redundant storage and erasure coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors. If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored.
Cross-Border Data Transfers and Location of Data	The FI should consider the social, political, and economic climate of a jurisdiction before an FI agrees to have its data stored or processed there. FIs should at the outset obtain legal advice to ascertain that the CSP is operating in jurisdictions that generally uphold confidentiality clauses and agreement.	Tencent Cloud's infrastructure spans multiple global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an independent fault isolation domain with physical separation. Customers can flexibly deploy data and systems across different regions or zones based on business needs and data security requirements to meet disaster recovery objectives. Tencent Cloud operates four data centers in Singapore, offering a wide range of cloud services including cloud servers, cloud databases, and CDN. Singapore customers can choose to store and process their data locally within Singapore.

No.	Domain	Summary of Controls
		Tencent Cloud adheres to principles of transparency. Upon request, Tencent Cloud will promptly provide information through appropriate channels regarding data storage locations, cold backup status, and backup storage locations. Tencent Cloud strictly complies with privacy and data protection laws and regulations in the jurisdictions where it operates. Tencent Cloud offers online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, which clearly define the scope and level of services provided, protection of user data and intellectual property.
Audit and Inspection	CSP should provide reasonable access to necessary information to assist in any FI investigation arising from an incident in the cloud or audit inspection.	Tencent Cloud will provide dedicated assistance and actively cooperate with customers and the Monetary Authority of Singapore (MAS) in audits and supervisory reviews as required. Tencent Cloud responds promptly to customer requests to support MAS-related inspections and compliance reviews.
Business Continuity Management	(a) Prior to contracting with the CSP, verify that the CSP has satisfactory business continuity plans ("BCP") and can recover the outsourced systems and/or IT services within the stipulated Recovery Time Objective ("RTO"). (b) FIs should ensure the CSP and FI regularly test its BCP and that the tests validate the feasibility of the RTO, Recovery Point Objective ("RPO") and resumption operating capacities; and (c) Ensure that plans and procedures are in place to address adverse conditions or termination of the outsourcing arrangement to allow the FI to continue business operations.	Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, certified to ISO/IEC 22301 international standards. To ensure service availability, Tencent Cloud conducts business impact analyses to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and develops disaster recovery strategies and continuity plans accordingly. Detailed contingency plans are established for cloud products and critical processes, and regular continuity drills are performed to validate their effectiveness.

No.	Domain	Summary of Controls
Third Party Risk Management	Third Party Risk Management - The CSP should be able to demonstrate that it implements and maintains a robust risk management and governance framework that effectively manages the cloud service arrangements including any sub-contracting arrangements.	Tencent Cloud enforces strict vendor security assessments, periodic monitoring, annual evaluations, independent reviews, and clear outsourcing agreements to ensure effective supplier management.
Subcontractors	Where a CSP elects to use subcontractors to perform the services which have a material impact to the provision of the cloud service, the FI and the CSP should agree on an appropriate notification method for changes in material subcontracting for the FI to exercise oversight.	Tencent Cloud publishes the online **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, and other legal documents on its international portal. For sub-processing scenarios, these agreements expressly set out clauses on prior consent to sub-processing, advance notice of any addition or replacement of sub-processors, and data-protection obligations. Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the relevant contract/agreement without the customer's prior written consent. Any anticipated change involving the addition or replacement of a sub-processor will be notified to the customer by e-mail or other agreed channels. Customers may also elect to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Regarding sub-contractor management, Tencent Cloud maintains a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers 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 the Monetary Authority of Singapore and financial institutions. In addition, Tencent Cloud actively cooperates with customers' outsourcing-management requirements and responds to and participates in audits or assessments initiated by customers.

No.	Domain	Summary of Controls
Default Termination	Refer to the MAS outsourcing guidelines for details on default termination and early exit.	If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Tencent Cloud supports data migration using standard formats and the same transmission methods as during onboarding, including **Direct Connect (DC)** and **VPN Connection**, services, to ensure secure and reliable data transfer. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored.
Exit Plan	The extent of exit planning should depend on the materiality of the outsourcing arrangement and potential impact to the on-going operations of the FI	
Shared Responsibility	The CSP and the FI should agree on the operational contract management, SLA management, technology risk management, business continuity management and contract exit	Tencent Cloud embraces the openness and shared nature of cloud computing services, continuously enhancing platform security and collaborating with customers to build a robust security framework. Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Considering that control responsibilities vary across service models (IaaS, PaaS, SaaS), Tencent Cloud has established a Shared Responsibility Model, detailed in Section 3 "Tencent Cloud Security Responsibility Sharing Model". Based on this model, Tencent Cloud works closely with customers to address security challenges collaboratively. 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.

12.2 Key Controls Recommended when Entering into a Cloud Outsourcing Arrangement

No.	Domain	Summary of Controls	Tencent Cloud's Response
A Govern the Cloud			
1	Organizational Considerations for the Management of Cloud Service Providers	Fis should consider adapting their organizational structure to ensure effective and timely oversight of CSPs for their performance, operational effectiveness of controls and remediation.	Customers should effectively and promptly monitor the performance, control measures, and operational effectiveness of cloud service providers. Tencent Cloud will provide dedicated assistance and actively cooperate with customers and the Monetary Authority of Singapore (MAS) in audits and supervisory reviews as required. 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. Tencent Cloud provides a ticketing system through its official console, enabling customers to report issues related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism. If frontline technical teams cannot resolve the issue effectively, the system automatically triggers an escalation process, involving product or technical teams to ensure timely resolution of customer requests or feedback. In addition, Tencent Cloud offers online chat and telephone support via the cloud console and official website, allowing customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates geographically redundant customer service centers, providing

No.	Domain	Summary of Controls	Tencent Cloud's Response
			24/7 support to handle customer requests, deliver round-the-clock technical assistance for cloud products, and ensure timely, high-quality service responses. Customers may also select an appropriate support plan, which can include access to dedicated support groups, a designated technical account manager, and value-added services for enhanced assistance.
2	Control Assessment & Monitoring	The FI should establish an appropriate control framework to manage the risks associated with the intended workloads and define the controls to meet corporate policies and regulatory. Risk assessment should assess the general security of the CSP and specific services to ensure required controls are implemented and operating within acceptable thresholds.	Customers should perform risk assessments on the overall security and services of cloud service providers to manage risks associated with anticipated workloads. 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 cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Singapore financial regulations, Tencent Cloud engages third-party audit firms annually to perform independent audits of its internal control framework and issues the Outsourced Service Provider Audit Report (OSPAR) in accordance with the Singapore Bankers Association standards. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3	Cost Management	With a distributed model of consumption, FI should track usage to ensure clear ownership of costs and facilitate internal distribution of these expenses.	Customers should track their cloud usage, including computing, storage, and network resources, to promote overall transparency in cloud utilization. Customers can view detailed information on resource consumption, billing statements, cost analysis, and reports for their account through the Billing Center in the Tencent Cloud console.
B Design & Secure the Cloud			
1	Cloud Architectural Reference Solutions & Practices	Design and implement cloud services which are optimized. Create a service catalogue of cloud products that adhere to the FI′ s internal policies and regulatory requirements.	Customers should establish a cloud service catalog that aligns with their business requirements, internal policies, regulatory obligations, and security standards, and design and implement optimized cloud services. Tencent Cloud's Financial Technology Solutions provide end-to-end support for digital transformation across multiple financial sectors, including consumer finance, payments, and fintech services. These solutions cover the entire business process, offering capabilities such as customer acquisition and marketing, financial risk control, intelligent customer service, scenario innovation, and cloud infrastructure services. Tencent Cloud remains committed to strengthening compliance and security while enabling financial business growth. Tencent Cloud offers service plans tailored to customer size and business needs, including Developer, Business, and Enterprise-level plans, providing unique tools and expertise to maximize the success of customers' businesses, products, and service
2	Virtualization, Containerization and DevOps	Manage the confidentiality and integrity risks associated with data co-mingling or shared tenancy environments. If a software or hardware fails, ensure that information assets remain secure or are securely removed.	Customers should manage confidentiality and integrity risks in mixed or multi-tenant environments. When software or hardware failures occur, information assets must be securely erased. In addition, customers should define standard tools and processes for managing containers, images, and deployments. Tencent Cloud provides **Cloud Virtual**

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Define a standard set of tools and processes to manage containers, images and release management.	Machine (CVM) services—scalable virtualized computing resources that allow customers to customize CPU, memory, storage, network, and security configurations. To ensure CVM security, customers can configure security groups and network ACLs to define access policies. Tencent Cloud also offers security services such as DDoS protection, DNS hijacking detection, intrusion detection, vulnerability scanning, web shell detection, and login protection. For container image management, Tencent Cloud Container Registry (TCR) provides secure, dedicated, high-performance image hosting and distribution services, including image security scanning, permission management, and access control for public and private networks, fully integrated with Cloud Access Management (CAM). Customers can also use Tencent Cloud Container Security Service (TCSS) for container asset management, image security scanning, runtime intrusion detection, and security baseline configuration, helping customers build a robust container security framework. Tencent Cloud implements appropriate technical and administrative measures—such as hardware virtualization, software isolation, and permission controls—to ensure tenant isolation in virtual environments, including separation between public and dedicated virtual machines. **To secure container environments**, Tencent Cloud has established a multi-layered container security architecture. For north-south traffic (between container cloud and external networks), Tencent Cloud leverages traditional security capabilities such as Web Application Firewall (WAF), DDoS protection, web vulnerability scanning, and Intrusion Detection and Prevention Systems (IDPS). For east-west traffic (within the container cloud), Tencent Cloud applies container-native security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			mechanisms based on principles such as security by design, shift-left security, and zero trust, implementing layered protections across infrastructure, container platform, and application layers. When media used to provide Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud follows strict procedures for complete physical destruction. For more details on virtualization and container management, refer to Section 7.9 Data and Infrastructure Security, **Clause 11.4 Virtualization Security.**
3	Resiliency in Cloud Architectures	FIs need to carefully consider and plan their cloud adoption to ensure that the resiliency and availability of the cloud services commensurate with their needs.	Customers should plan cloud application strategies to ensure resilience, recoverability, and availability consistent with their requirements. Tencent Cloud builds or leases data centers worldwide in compliance with international standards and local security requirements, offering multi-region and multi-zone options to meet disaster recovery and service level objectives. Tencent Cloud's compute, network, storage, database, container, middleware, and security services are designed for high availability and include disaster recovery plans. To support regulatory compliance, Tencent Cloud's global data centers feature multiple carrier connections at each availability zone, enabling cross-region disaster recovery capabilities and reducing the impact of public network failures. Regions are fully isolated from each other, and each region is subdivided into multiple isolated availability zones to maximize stability and fault tolerance. This multi-zone design minimizes single-point failures and ensures business continuity. Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point device

No.	Domain	Summary of Controls	Tencent Cloud's Response
			failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability. For more details on business continuity, refer to Section 7.6 "IT Resilience" and Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management."
4	Network Architectures	FI should plan and implement security controls to secure the cloud workload against common internet-based attacks and cloud-specific attacks.	Customers should implement necessary security controls to protect cloud workloads from Internet-based attacks. Tencent Cloud provides the **Virtual Private Cloud (VPC)** service, which enables complete isolation between private networks and offers customers an independent and secure cloud network environment. In addition, Tencent Cloud offers a range of security products to help customers establish strong perimeter defenses, including **Web Application Firewall (WAF)**, **Cloud Firewall (CFW)**, **VPN Connection**, and **Anti-DDoS**. Tencent Cloud has deployed a mature network security architecture that incorporates multiple layers of defense, including firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS protection, network segmentation, and web application security, to mitigate Internet threats. Tencent Cloud also enforces strict access control policies at the virtualization layer, isolation strategies for internal private networks, role-based permissions for the web console, and secure mechanisms such as session IDs and access keys to ensure that each customer can only access their purchased resources, effectively achieving multi-tenant isolation. For more details on network security, refer to Chapter 7.9 "Data and Infrastructure Security," Section 11.2 "Network Security."

No.	Domain	Summary of Controls	Tencent Cloud's Response
			For more details on network security, refer to Section 7.9 Data and Infrastructure Security, Clause 11.2 Network Security.
5	Cryptographic Key Management	Manage cryptographic material so that the confidentiality and integrity of the FI ' s data is not compromised.	Customers should implement security measures to strengthen encryption material management, such as regular key rotation, lifecycle management, and secure backup, to ensure data confidentiality and integrity. To assist customers in protecting the confidentiality, integrity, and availability of keys, Tencent Cloud provides the **Key Management Service (KMS)**, which enables customers to easily create and manage keys for multiple applications and business scenarios in compliance with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, simplifying encryption implementation. Tencent Cloud has established encryption and key management standards covering key application, generation, storage, usage, transmission, update, and destruction processes to ensure confidentiality, integrity, and availability. For more details on key management, please refer to Section 7.8 "Cryptography," **Clause 10.2 "Key Management"**.
6	Encryption	Provide assurance that only authorized parties can gain access to the data in transit and at rest. Provide assurance that the confidentiality and/or integrity of the data has not been compromised. Provide authentication of source and non-repudiation of message	Customers should ensure that only authorized personnel can access data in transit and at rest and implement necessary management measures to maintain confidentiality and integrity. To protect stored data, Tencent Cloud's storage and database products support encryption using strong algorithms and integrate with **Key Management Service (KMS)** for full lifecycle key management. KMS uses FIPS 140-2 certified Hardware Security Modules (HSMs) to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			generate and protect keys, supporting complete key lifecycle management. **For data transmission protection**, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide 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.
8	User Access Management and Authentication	The full life cycle of user access management should be considered when implementing a cloud outsourcing arrangement. This includes the definition of identity and access management requirements, approval, provisioning, credential management, access review and revocation.	Customers should manage user access throughout its lifecycle to ensure adherence to the principle of least privilege and implement segregation of duties for sensitive roles to protect data confidentiality and integrity. Tencent Cloud provides **Cloud Access Management (CAM)** to help customers securely and precisely manage access to Tencent Cloud products and resources. The primary account by default has full access to resources under its ownership and can create sub-users, assign identity IDs, credentials, and permissions. CAM also supports activity monitoring through **CloudAudit**, enabling compliance checks, operational reviews, and risk assessments for Tencent Cloud account activities.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			To support customers in meeting regulatory requirements, Tencent Cloud has established internal access control standards that mandate the use of unique identifiers for user accounts and enforce password policies based on security baselines. Tencent Cloud employs a zero-trust security management system for employee access authentication, requiring users to log in and complete multi-factor authentication before accessing internal resources. Tencent Cloud also maintains authorization policies and a role-based segregation matrix, recording personnel identity information and corresponding permission levels for each business system. Regular internal permission reviews are conducted to prevent misuse or abuse of privileges. Tencent Cloud enforces strict internal network isolation rules, ensuring complete separation between its corporate network and the production environment where customer data resides through physical and logical isolation. Bastion hosts are fully deployed in the production environment to prevent unauthorized access.
9	Privileged User Access Management	The FI should ensure that privileged accounts are managed so that the CSP should only have access to its information assets by authorized exception.	Customers should manage privileged accounts to ensure that the cloud service provider can only access information assets under authorized exceptional circumstances. Tencent Cloud provides **Cloud Access Management (CAM)**, which allows customers to assign resource permissions to sub-users using tags, enabling fine-grained access control over cloud resources. CAM also supports operational auditing through **CloudAudit**, which facilitates compliance monitoring, operational reviews, and risk assessments of Tencent Cloud account activities. In addition, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			access assets and perform their tasks. Bastion Host also supports operation auditing by recording and analyzing user activity logs to ensure effective traceability of security events. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. If customers encounter any issues related to accounts, network security, or product usage, they can submit a support ticket through the console to obtain technical assistance. Tencent Cloud has implemented comprehensive operational security measures to ensure that service teams cannot directly access customer information assets without explicit consent and authorization. To further support regulatory compliance, Tencent Cloud maintains complete isolation between its internal corporate network and the production environment where customer data resides. Operations personnel must access the production environment through Bastion Host, and all operational accounts are equipped with multi-factor authentication. When granting permissions, Tencent Cloud applies fine-grained privilege segmentation to ensure that employees receive only the minimum permissions required to deliver the relevant service. Requests for additional permissions must undergo multi-level review and approval. All backend operational activities are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these records to ensure compliance and security.
10	Administrative Remote Access	Provide assurance that remote access to systems is secured against threats of impersonation. Provide assurance that user management controls are	Customers should manage remote access to platforms and systems within their cloud environments, and cloud service providers should also manage remote access to their own systems. To enable customers to securely and quickly

No.	Domain	Summary of Controls	Tencent Cloud's Response
		present and monitored for suspicious activity.	access cloud business systems anytime, anywhere, and from any mainstream device, Tencent Cloud supports SSL VPN technology for remote access. SSL VPN encrypts data transmitted over the Internet to ensure security and provides access control mechanisms to reduce unauthorized access. Customers can also use **VPN Connection** to establish secure communication between their on-premises data centers and Tencent Cloud resources. The VPN tunnel uses Internet Key Exchange (IKE) and IPsec protocols to encrypt transmitted data, creating a secure and trusted data tunnel over the Internet. The VPN gateway is highly reliable, built on a master/slave hot backup architecture, ensuring uninterrupted communication sessions and seamless failover that is imperceptible to upper-layer applications. If customers encounter any issues related to accounts, network security, or product usage, they can submit a support ticket through the console to obtain technical assistance. Tencent Cloud provides comprehensive operational security measures to ensure that service teams cannot directly access customer information assets without explicit consent and authorization. Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect through encrypted communication channels to access Tencent Cloud's corporate network and office systems remotely. Tencent Cloud maintains remote access logs to record user activities. Furthermore, Tencent Cloud's internal office network is completely isolated from the production environment where Customer data resides. When Tencent Cloud employees are authorized by customers to access customer information assets, they must use a bastion host to enter the production

No.	Domain	Summary of Controls	Tencent Cloud's Response
			environment. All operations are performed using accounts with multi-factor authentication. When granting permissions, Tencent Cloud enforces fine-grained access controls to ensure employees receive only the minimum privileges necessary to deliver the required service. Requests for additional permissions must undergo multi-level review and approval. All backend maintenance operations are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these records.
11	Data Loss Prevention	The FI should have in place a holistic data loss prevention strategy which includes data in transit, at rest and end point security controls.	Customers should establish data loss prevention strategies to protect data processed and stored in the cloud environment and prevent unauthorized or accidental disclosure. 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. Tencent Cloud has also implemented real-time monitoring and interception mechanisms to detect and block any abnormal data access behavior. In addition, Tencent Cloud deploys Data Loss Prevention (DLP) tools on employee computers to effectively restrict data export and monitor, detect, and prevent potential data theft activities. For more information on Tencent Cloud data security, please refer to Section 7.9 "Data and Infrastructure Security," **Clause 11.1 "Data Security"**.
12	Source Code Reviews	Ensure confidentiality and integrity of source codes, other code artefacts. Prevent unauthorized alteration of code and system configurations.	Customers should review source code to ensure the confidentiality and integrity of source code and other code components. Tencent Cloud's **Cloud Native Build (CNB)** provides a complete developer toolchain, including code hosting, high-performance CI/CD pipelines, AI code assistant, and artifact management. The AI code assistant, designed specifically for developers, supports multiple mainstream programming languages and offers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			features such as code completion, unit testing, code diagnostics, intelligent reviews, and smart Q&A for code issues—helping developers improve coding quality and efficiency. Tencent Cloud has established detailed secure coding guidelines that internal developers must strictly follow. Tencent Cloud provides secure programming training to enhance developers' awareness of risks such as injection attacks and sensitive data leaks. During development, developers are required to consider security features within application systems to minimize vulnerabilities. Tencent Cloud's internal code security analysis framework integrates capabilities such as Static Application Security Testing (SAST), open-source component scanning, and sensitive information detection. Business teams can leverage pipeline-based self-service scanning during the code admission phase to perform security assessments. Typical issues identified during code reviews are documented and consolidated into the team's knowledge base. Code review standards cover detection of vulnerabilities such as XSS, SQL injection, code execution, command injection, historical vulnerabilities in third-party components, and sensitive information protection. **For application security scanning**, Tencent Cloud requires business teams to connect web application test environments to web vulnerability scanning tools for automated scanning before product launch. If vulnerabilities are detected, tickets are automatically generated and assigned to the responsible development team for remediation prior to release, ensuring security issues are not carried into production. For more details on secure coding, source code review, and application security testing, refer to Section 7.4 "System Development Life Cycle and Security-By-Design," **Clause 6.1 "Secure**

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Coding, Source Code Review, and Application Security Testing."
13	Penetration Testing	Using regular vulnerability assessments and periodic penetration tests, identify vulnerable configurations and provide assurance as to the security posture of a service, and provide assurance of security processes including security patching and hardening	Customers should ensure that penetration testing reports from the cloud service provider can be used to gain assurance of the underlying system's security and that any identified vulnerabilities are properly assessed, tracked, and managed. Tencent Cloud's **Vulnerability Scanning Service (VSS)** leverages years of accumulated security expertise and threat intelligence to maintain a comprehensive vulnerability rule base and provides professional and efficient detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection on customer assets, assessing availability, security, and compliance. It also provides professional remediation recommendations to help customers reduce security risks. Tencent Cloud's **Cloud Pressure Testing (PTS)** simulates attack techniques and vulnerability exploitation methods that hackers might use, applying controlled and non-destructive approaches to thoroughly probe the security of target systems. PTS identifies weaknesses in targets and network devices and provides security hardening recommendations to help customers improve system security. Internally, Tencent Cloud has established a regular vulnerability scanning and penetration testing mechanism. Vulnerability scanning systems generate scheduled tasks to scan assets within the cloud environment, and any detected vulnerabilities are analysed, categorized, and remediated. Tencent Cloud's security team conducts large-scale end-to-end penetration tests periodically and performs targeted penetration tests before new product launches or major changes. Penetration test results are

No.	Domain	Summary of Controls	Tencent Cloud's Response
			communicated through security tickets to the responsible departments, which promptly patch vulnerabilities or implement compensating controls to ensure that exploitable weaknesses identified during testing are properly addressed. Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.
14	Security Events Monitoring	The monitoring of the cloud environment for security events and incidents should be centralized to provide the FIs a single pane of glass for situational awareness and incident response. Ensure log information are secured against unauthorized access and tampering.	Customers should implement centralized monitoring of security events and incidents within the cloud environment to ensure that security events are detected and responded to in a timely manner. Customers may use **Cloud Log Service (CLS)**, a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. The **Cloud Security Center (CSC)** aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Customers can also use CloudAudit to record logs and continuously monitor account activity across Tencent Cloud infrastructure. **Elasticsearch Service (ES)** enables customers to stream real-time logs from cloud servers, containers, and other cloud products, as well as ingest historical and incremental business data

No.	Domain	Summary of Controls	Tencent Cloud's Response
			into Tencent Cloud ES clusters for distributed storage and analytical queries. To support customers in meeting regulatory requirements, Tencent Cloud has established a Security Operations Center (SOC) built on cloud-native technologies, focusing on threat detection, investigation, and response to enhance operational efficiency and achieve full visibility, awareness, and control over the security posture of the entire network. The dedicated team operates 24/7, providing professional security operations, promptly intervening to handle security alerts, performing initial analysis, and formulating containment strategies to prevent attacks or security incidents from occurring. In addition, Tencent Cloud leverages years of experience in anomaly behaviour monitoring to maintain a comprehensive rule base that automatically triggers real-time alerts for abnormal activities. Tencent Cloud has also defined strict internal operational security "red lines" and conducts regular internal reviews to ensure compliance and prevent unauthorized actions.
15	Securing Logs and Backups	Log data should have robust controls to ensure their confidentiality and integrity. Log data should not contain sensitive information. Ensure the confidentiality and integrity of backup data.	Customers should implement necessary security measures to protect log data and backup data, ensuring their confidentiality, integrity, and availability. **For log management,** Tencent Cloud provides the **Cloud Log Service (CLS)** to assist customers in collecting, aggregating, and analysing event-related evidence. CLS is designed with a highly available distributed architecture and stores log data with multiple redundant backups to prevent data loss in the event of a single-node failure, ensuring service availability and reliability. In addition, Tencent Cloud's Elasticsearch Service (ES) is deployed within logically isolated Virtual Private Clouds (VPCs), allowing customers to fully control

No.	Domain	Summary of Controls	Tencent Cloud's Response
			their environment configurations, customize network access control lists and security groups, and leverage multi-availability zone deployment options to maintain service continuity even during network or power outages in a single zone. **For network log collection and retention**, Cloud Firewall (CFW) supports full traffic analysis and can retain logs for up to six months. It also provides advanced threat tracing capabilities, including analysis of domain registration, resolution, filing, and historical DNS information. For operation log collection and retention, customers can use CloudAudit to monitor Tencent Cloud account activities, perform compliance checks, and conduct operational and risk audits. CloudAudit supports online viewing of console and API operation records for up to 90 days. To support regulatory compliance, Tencent Cloud has established comprehensive log collection and management standards covering the recording, extraction, storage, protection, analysis, and auditing of login logs, operation logs, system logs, and security event logs. All logs are centralized on Tencent Cloud's log management platform and protected with strict backup and security measures to prevent unauthorized modification or deletion. Tencent Cloud uses automated operational security auditing tools and an internal audit team to review logs regularly, detect anomalies, and mitigate operational risks. **For backup management**, Tencent Cloud builds or leases data centers worldwide in compliance with international standards and local security requirements, offering customers multi-region and multi-zone options to meet disaster recovery and service level objectives. Tencent Cloud's compute, network, storage, database, container, and middleware services provide highly available architectures and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			support customer-defined backup strategies to meet diverse backup needs. Many Tencent Cloud products also support access control and encryption features to ensure the confidentiality and integrity of stored data and backup data. For more details on backup management, refer to Section 7.6 "IT Resilience", clause **"8.4 "System Backup and Recovery."**
C Run the Cloud			
1	Change Management	Ensure that all the changes follow a robust change management process. Ensure heightened oversight of major changes that could impact the stability and/or security of the cloud operating environment. Detection of unauthorized or erroneous changes.	Customers should ensure that all changes made by the cloud service provider follow established change management processes, strengthen oversight of major changes that may affect the stability or security of the cloud operating environment, and detect unauthorized or erroneous changes. To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive product and configuration change management standard that clearly defines each step of the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud has defined an emergency change management process, under which emergency changes can only proceed after appropriate approval. All types of program changes, including application and configuration file updates, operating system modifications, and database changes, must undergo business impact analysis, have rollback plans in place, and receive approval from designated responsible parties before deployment. Tencent Cloud's change release system enforces strict controls, requiring that change operations be executed only by authorized personnel and that all change-related logs be retained for regular audit. After a change is released, the requester must perform post-implementation functional acceptance testing, and Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Cloud monitors and records the change status in the production environment. For more details on incident detection, response, and communication, please refer to Section 7.5 IT Service Management, clause "**7.5 Change Management**."
2	Configuration Management	The configuration management of the software defined environment is critical for the safe and secure operations of the cloud and information assets. Prevent unauthorized changes to the cloud environment, and ensure such changes are detected and remediated to prevent high impact incidents.	Customers should also establish configuration management mechanisms to detect unauthorized changes in the cloud environment and implement corrective measures to prevent high-risk incidents. Tencent Cloud's **Cloud Security Center (CSC)** provides automated configuration risk assessment capabilities to help customers reduce security risks caused by misconfigurations and improve overall cloud security posture. Customers can also use **Config Audit** to perform centralized auditing and governance of cloud resources, continuously recording configuration details and changes across different regions under their account. Based on Tencent Cloud best practices and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. To support regulatory compliance, Tencent Cloud has established network security configuration standards and security baseline standards to standardize the configuration of network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud continuously scans operating systems, database management systems, and virtual images for deviations from established standards. When deviations are detected, Tencent Cloud automatically generates security tickets and assigns them to responsible teams for timely remediation. Tencent Cloud also conducts regular reviews of security policies and parameter settings for routers, firewalls, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			network servers to ensure their effectiveness.
3	Events Management	The CSP is usually responsible for events that impact the underlying infrastructure of the FIs workloads, which could include the virtual environment, containers, or customer workloads. Manage and escalate events appropriately according to their criticality and assigned ownership.	Customers should define and monitor critical events, detect network and system anomalies, and respond promptly to potential security incidents. Events should be managed and reported based on severity and assigned ownership. To support customers in detecting and responding to incidents quickly, Tencent Cloud provides a unified security management platform—**Cloud Security Center (CSC)**—which integrates asset management, risk management, alert management, and advanced security operations. CSC enables a closed-loop security process covering proactive threat detection, real-time incident response, and post-incident forensic analysis, improving overall security operations efficiency. Tencent Cloud has established a detailed incident management process and uses internal security operation systems to record security events. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as event type, data sensitivity, and impact scope, and promptly notifies the responsible parties for follow-up actions. Supported by a 24/7 security operations framework, Tencent Cloud focuses on vulnerability monitoring, intrusion tracing, and attack mitigation, responding to alerts in real time and quickly formulating containment and remediation strategies to prevent incident escalation. **For incident notification,** Tencent Cloud evaluates the impact and severity of security events and, after internal review, communicates the handling and analysis results to affected customers through appropriate channels, providing technical support to help customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			take remedial measures and minimize losses. **For customer-reported issues,** Tencent Cloud provides a ticketing system through the official console, allowing customers to report faults, incidents, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priorities through a tiered response mechanism, and if frontline teams cannot resolve the issue effectively, the system automatically triggers an escalation process involving product or technical teams to ensure timely resolution. **For continuous improvement,** Tencent Cloud has established a periodic incident analysis mechanism to conduct multi-dimensional reviews of incidents, including type, frequency, impact scope, and severity. Based on root cause analysis and post-incident reviews, Tencent Cloud implements preventive measures to avoid recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a detailed analysis report for management review. For more details on incident management, please refer to Section 7.5 IT Service Management, clause "**7.7 Incident Management**."
4	Incident and Problem Management	Timely detection of critical incidents coupled with tight integration with incident response and management processes can allow incidents to be remediated speedily, thereby limiting downtime or potential data breaches.	Customers should establish event and problem management mechanisms to ensure traceability of security incidents within the IT environment when new threat intelligence becomes available. Customers should also review incidents, implement corrective measures to address identified gaps, and prevent recurrence. Tencent Cloud has implemented a problem management framework that analyzes incident data and trends to identify root causes and develop solutions, minimizing the impact of incidents and problems on business operations. In addition, Tencent Cloud maintains centralized knowledge management for problem resolution to improve handling efficiency and

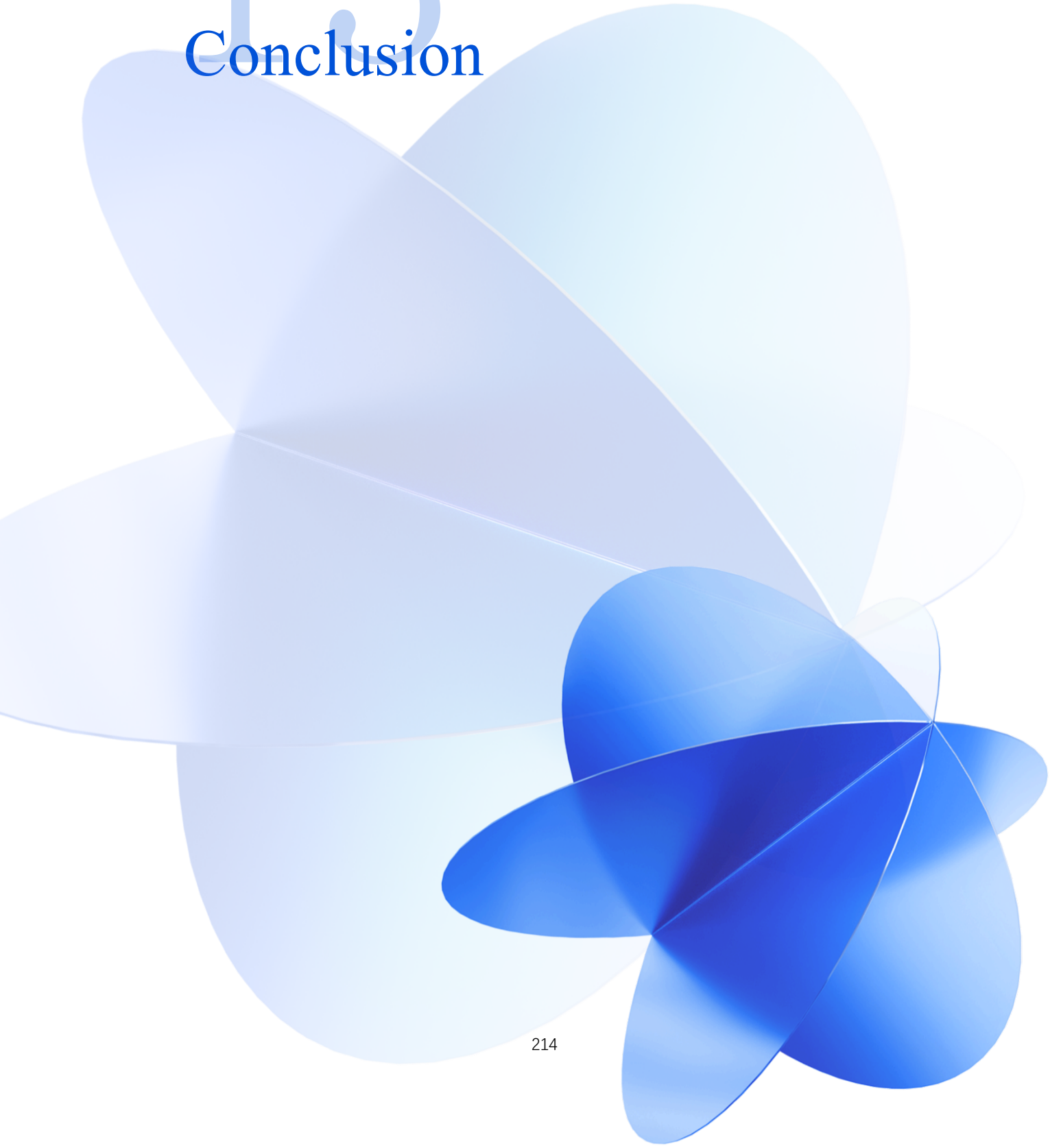
No.	Domain	Summary of Controls	Tencent Cloud's Response
			applies preventive measures to avoid repeated occurrences, thereby enhancing service quality. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews of incidents, including type, frequency, impact scope, and severity. Based on post-incident reviews and root cause analysis, Tencent Cloud implements preventive measures to reduce the likelihood of similar incidents. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a detailed analysis report for management review.
5	Capacity Management	The FI should have a clear view of its requirements to operate its resources to ensure that business functions can proceed without any interruptions. Resources are monitored appropriately to understand average utilization and peaks.	Customers should establish a capacity management mechanism to understand their operational resource requirements and monitor their cloud resources to ensure smooth business functionality. To enable effective monitoring and management of system performance, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services.
6	Patching and Vulnerability Management	FIs need to detect and remediate the vulnerabilities in the cloud environment swiftly.	Customers should establish vulnerability and patch management mechanisms to detect and remediate vulnerabilities in the cloud environment and to deploy security and operating system patches. **To assist customers with vulnerability remediation and asset risk management**, Tencent Cloud provides **Cloud Security Center (CSC)**. CSC enables one-stop security management for cloud assets, including automated asset inventory, detection and identification of various asset security risks, and automated response and remediation. Leveraging Tencent's threat intelligence capabilities, CSC pushes the latest vulnerability information to customers and provides detailed vulnerability reports, including impact scope and remediation recommendations, enabling rapid awareness and timely handling of high-risk vulnerabilities. CSC also supports automated orchestration so customers can preconfigure automated response and remediation playbooks to improve threat response efficiency. For container vulnerability remediation and management, **Tencent Cloud Container Security Service (TCSS)** can scan on-premises and registry images on a regular or on-demand basis, retrieve vulnerability information from authoritative sources in real time, and update its vulnerability database daily. TCSS supports Tencent Cloud's vulnerability exploitation

No.	Domain	Summary of Controls	Tencent Cloud's Response
			defense system, a virtual patching capability developed to protect against frequently emerging zero-day vulnerabilities. By integrating Tencent's vulnerability research and high-severity real-time alerting capabilities, TCSS generates virtual patches that automatically take effect on cloud servers, effectively blocking malicious exploitation attempts. To support customers in meeting regulatory requirements, Tencent Cloud identifies newly released patches and conducts sufficient security testing prior to installation to ensure patch safety. Tencent Cloud regularly notifies internal business teams to perform patch upgrades and installations, uses endpoint detection tools to regularly scan patch deployment status, and automatically generates alert tickets for devices that exceed patching deadlines.
7	Collaborative Disaster Recovery Testing	The outsourcing arrangement should contain Business Continuity Planning (BCP) requirements on the CSP, ensure the continued availability of services commensurate with their criticality in the cloud environment.	Customers should plan and conduct disaster recovery testing to ensure that data, systems, and applications can be restored within the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Tencent Cloud builds or leases data centers worldwide in accordance with international standards and local security requirements, providing multi-region and multi–availability zone options to meet disaster recovery requirements and service level objectives. Tencent Cloud's compute, network, storage, database, container, middleware, and security services are designed for high availability and are supported by corresponding disaster recovery plans. To support regulatory compliance, Tencent Cloud regions are fully isolated from one another to maximize stability and fault tolerance. Each region is further divided into multiple isolated availability zones to enhance data availability and reduce single

No.	Domain	Summary of Controls	Tencent Cloud's Response
			points of failure, thereby ensuring business continuity for customers. Tencent Cloud is certified to the ISO/IEC 22301 Business Continuity Management System international standard. Tencent Cloud performs business impact analyses for its cloud products and services and based on the analysis results, formulates response strategies, business continuity plans, and disaster recovery plans to guide the restoration of relevant business resources. Detailed disaster recovery runbooks are defined for cloud products, and regular exercises are conducted in strict accordance with requirements to validate timeliness and feasibility. For more details on business continuity, refer to Section 7.6 "IT Resilience" and Section 9: "How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines on Business Continuity Management."

13 Conclusion



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

This guide is based on key regulatory requirements issued by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS). It aims to provide customers with a comprehensive and transparent overview of how Tencent Cloud supports compliance for cloud-hosted systems and data, helping enterprises confidently and securely migrate their systems and data to the cloud. Through this guide, Tencent Cloud seeks to assist enterprise customers in effectively meeting regulatory compliance standards while achieving digital innovation and business growth.

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

14 Version History



Date	Version	Detail
April 2016	V1.0	Initial Release