Tencent Cloud

Tencent Cloud User Guide to Financial Industry Regulations & Guidelines in Hong Kong Special Administrative Region of the People's Republic of China

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 intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

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 TM-G-1

5.1 IT Control Governance 17
5.2 Protection 18
5.3 System Development and Change Management 28
5.4 Information Processing 31
5.5 Communications Networks 34
5.6 Management of Technology Service Providers 38

06 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2

07 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of SA-2

08 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-E-1

09 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Practice Guide on Cloud Adoption

9.1 Governance and Oversight 80
9.2 Risk Assessment and Due Diligence 81
9.3 Cloud Service Provider Contractual Provisions and Related Controls 88
9.4 Cloud Resilience and Exit Strategy 91
9.5 Cloud Security and Data Protection 94
9.6 Incident Management 114
9.7 Ongoing Monitoring 117
9.8 Workforce Strategy and Empowerment 121

10 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guideline on Authorization of Digital Banks

11 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Customer Data Protection

12 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Incident Response

CONTENTS

and Management Procedures

12.1 Incident Detection and Rapid Response 135
12.2 Communication Strategy and Notification Procedure 135

13 Conclusion

14 Version History

01 Overview



The Hong Kong Monetary Authority (HKMA) has issued a series of Supervisory Policy Manuals (SPMs), guidelines, and circulars to govern the financial industry. Adopting a risk-based supervisory approach, the HKMA assesses the safety and soundness, risk management frameworks, and internal control measures of Authorized Institutions (AIs)[1] to ensure effective supervision.

At the same time, to enhance the competitiveness of Hong Kong's financial and banking sectors, the HKMA has introduced various initiatives to encourage AIs to pursue technological innovation and digital transformation, ushering Hong Kong into a new era of Smart Banking.

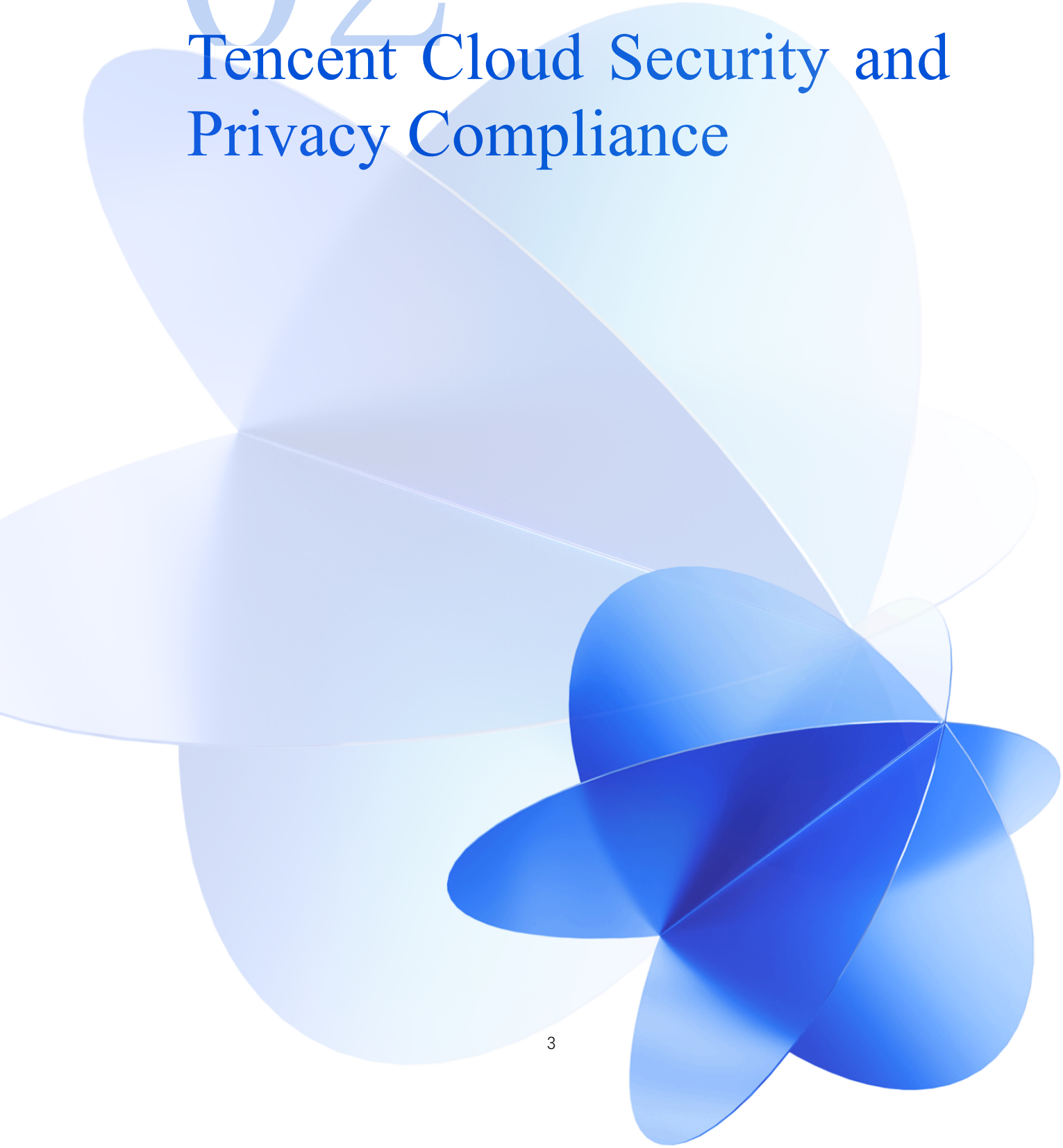
Given the increasing adoption of cloud computing by AIs in recent years, the HKMA expects institutions to effectively manage associated risks when leveraging such technologies. This includes ensuring compliance with existing regulatory requirements, particularly those related to technology risk management and outsourcing arrangements:

- TM-G-1 General Principles for Technology Risk Management
- TM-G-2 Business Continuity Planning
- SA-2 Outsourcing
- TM-E-1 Risk Management of E-banking
- Practice Guide on Cloud Adoption
- Guideline on Authorization of Digital Banks
- Guidance on Cloud Computing
- Customer Data Protection
- Incident Response and Management Procedures

[1] An authorized institution is a bank, restricted license bank, or deposit-taking company authorized by the HKMA to carry on the business of taking deposits.

02

Tencent Cloud Security and Privacy Compliance



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

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

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

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

2.1 Global Compliance

CSA STAR Certification	The CSA STAR cloud security assessment is an international certification launched by the Cloud Security Alliance (CSA), a globally recognized non-profit organization. It extends the ISO/IEC 27001 Information Security Management System and incorporates the Cloud Control Matrix (CCM), visualizing cloud-specific security challenges and providing users with a clear overview of security architecture evaluation. Leveraging years of accumulated security practices, Tencent Cloud has obtained the CSA STAR Gold Certification, demonstrating that its security governance framework meets internationally recognized cloud security standards.
SOC Audit	System and Organization Controls (SOC) Reports are a series of internal control reports for service organizations issued by professional third-party accounting firms in accordance with the standards of the American Institute of Certified Public Accountants (AICPA). As independent audit reports, SOC Reports cover control points related to security, availability, and confidentiality of the Tencent Cloud platform. Depending on the type of attestation service, SOC Reports can be provided to cloud users and their auditors, offering valuable information to help assess and address risks associated with the service organization.

2.2 ISO/IEC Certification

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

	Tencent Cloud has obtained ISO/IEC 22301:2019 certification, demonstrating that it has established formal business continuity management processes to ensure operational stability and resilience.
ISO/IEC 27001: 2022 Certification	ISO/IEC 27001:2022 Information Security Management System is recognized globally as one of the most authoritative, rigorous, and widely adopted certification standards in the field of information security. Achieving this certification signifies that an organization has established a scientific and effective information security management framework to align business strategy with security governance, ensuring that information security risks are properly controlled and addressed. Obtaining ISO/IEC 27001:2022 certification further demonstrates Tencent Cloud's commitment to security and confirms its capability to deliver secure and reliable cloud products and services.
ISO/IEC 20000-1: 2018 Certification	ISO/IEC 20000-1:2018 is an international standard for IT Service Management (ITSM). It defines a structured approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving IT service management systems. The standard helps organizations consistently identify and manage IT-related issues, strengthen communication with users, and build a standardized service framework that supports continuous improvement. Tencent Cloud has obtained ISO/IEC 20000-1:2018 certification, covering cloud computing services, hosting services, and disaster recovery services, demonstrating its commitment to delivering reliable and customer-focused IT service management.
ISO/IEC 9001: 2015 Certification	ISO 9001:2015 is a globally recognized and mature quality management system standard. It provides a comprehensive framework and guiding principles for managing the entire life cycle of products and services, ensuring consistent and stable delivery quality. Tencent Cloud has obtained ISO 9001 certification, covering cloud computing services, hosting services, and disaster recovery services. By implementing a quality management system, Tencent Cloud effectively achieves its quality objectives and ensures the reliability and operational excellence of its cloud products and services.
ISO/IEC 27017: 2015 Certification	ISO/IEC 27017:2015 is an international standard that supplements ISO/IEC 27002:2013, providing practical guidelines for cloud service information security. It offers specific security controls and implementation guidance for both cloud service providers and customers, strengthening the management of threats and risks unique to cloud computing environments. Tencent Cloud has obtained ISO/IEC 27017:2015 certification, demonstrating its adherence to internationally recognized best practices and its commitment to building a comprehensive cloud security management system that enhances overall cloud security capabilities.
ISO/IEC 27018: 2014 Certification	ISO/IEC 27018:2014 is a globally recognized standard for the protection of personally identifiable information (PII) in public cloud environments. It provides a set of best practices for cloud service providers to safeguard user privacy and ensure the security of personal data in cloud computing. Tencent Cloud has obtained ISO/IEC 27018:2014 certification, signifying that its personal information management system complies with stringent international requirements for personal data protection, offering customers greater trust and assurance in cloud security.

ISO/IEC 29151: 2017 Certification	ISO/IEC 29151:2017 is an international standard that defines control objectives, controls, and implementation guidelines for processing personally identifiable information (PII) to address risks and privacy requirements identified through risk and impact assessments. Tencent Cloud has obtained ISO/IEC 29151:2017 certification, demonstrating that it has developed an appropriate security control framework based on its PII objectives and business needs, providing a high level of privacy protection for user PII in the cloud.
ISO/IEC 27701: 2019 Certification	ISO/IEC 27701:2019 is an extension of ISO/IEC 27001 and ISO/IEC 27002, providing requirements and guidelines for establishing, implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). It represents a significant milestone in the ongoing management of privacy risks. Tencent Cloud has obtained ISO/IEC 27701:2019 certification, demonstrating that user privacy protection is a core element of its services and confirming the standardization and reliability of privacy protection across Tencent Cloud products.

2.3 Regional and Industry Compliance

C5 [Germany]	The Cloud Computing Compliance Criteria Catalogue (C5) was developed by the German Federal Office for Information Security (BSI) to verify the information security compliance of cloud service providers through standardized audits and reporting. C5 is widely recognized as a high-level security standard in the cloud services industry. Tencent Cloud has passed the German C5:2020 basic and additional audit criteria, demonstrating that its data protection and information security practices meet the stringent requirements set by the German government.
TISAX [Germany]	TISAX (Trusted Information Security Assessment Exchange) is an information security assessment and data exchange standard jointly launched by the German Association of the Automotive Industry (VDA) and the European Network Exchange (ENX). It enables mutual recognition of information security assessments within the automotive industry and provides a unified evaluation and exchange mechanism. Multiple Tencent Cloud Internet Data Centers (IDCs), including those located in Beijing and Shenzhen, have passed TISAX Level 3 assessments, ensuring that all services deployed in these regions meet TISAX requirements and maintain a robust information security management system.
MTCS Tier3 [Singapore]	The Multi-Tier Cloud Security (MTCS) Standard was developed under the guidance of the Infocomm Development Authority of Singapore (IDA) and its Information Technology Standards Committee (ITSC). As a widely adopted cloud security standard, MTCS helps cloud service providers address customer concerns regarding data security, confidentiality, and the impact of cloud services on business operations. Tencent Cloud has obtained MTCS Level 3 certification, indicating that it has implemented robust risk management mechanisms to ensure data security, confidentiality, and verifiable operational transparency for its cloud customers.
OSPAR [Singapore]	The Outsourced Service Provider's Audit Report (OSPAR) is the outsourcing compliance standard for the Singapore financial industry. Based on the Singapore Standards on Assurance Engagement (SSAE 3000), it verifies the

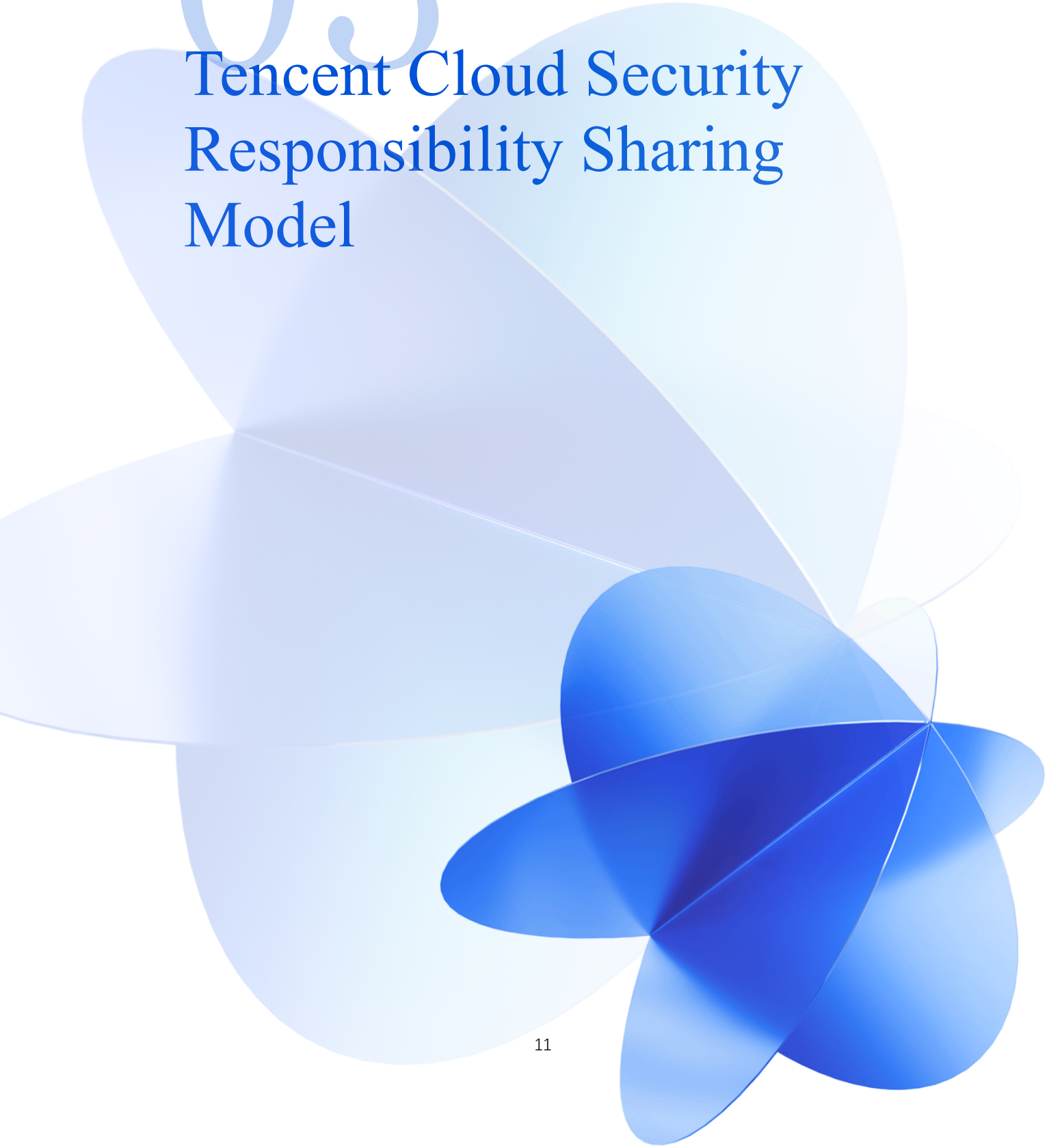
	design and operational effectiveness of controls in three areas: entity-level controls, general IT controls, and service controls. Tencent Cloud has obtained OSPAR attestation for multiple products and services in the Singapore region, demonstrating that its security capabilities meet the stringent requirements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

financial industry	obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure.
IT compliance audit in Thailand financial industry	Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange Commission (OSEC), the Office of Insurance Commission (OIC), and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's compliance with Thailand's stringent financial industry regulatory requirements and its commitment to providing high-quality, compliant cloud services to financial sector customers.
IT compliance audit in Indonesian financial industry	Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan, OJK), and other Indonesian financial regulatory authorities have issued regulations for the financial services industry. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits confirm that Tencent Cloud strictly complies with the regulatory requirements of Indonesia's financial industry when providing cloud services to financial customers.
IT compliance audit in Philippines financial industry	Financial institutions in the Philippines are required to comply with regulations issued by the Bangko Sentral ng Pilipinas (BSP) and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's ability to comply with the stringent regulatory requirements of the Philippine financial industry and its commitment to providing high-quality, compliant cloud services to financial sector customers.
The Motion Picture Association of America (MPAA)	The Motion Picture Association of America (MPAA) has established a set of best practice standards for securely storing, processing, and transmitting protected media content. This implementation guidance is intended to help application and cloud service providers working with MPAA members understand the requirements for content security. The components of the MPAA Content Security Model reference relevant ISO standards (ISO 27001 and ISO 27002), recognized security standards (such as NIST, CSA, ISACA, and SANS), and industry best practices. Tencent Cloud has obtained certifications including ISO 27001, ISO 27017, ISO 27018, PCI DSS, and CSA STAR, and has conducted self-assessments to ensure that its content management processes comply with the MPAA Content Security Model.
HIPAA [US]	Health Insurance Portability and Accountability Act (HIPAA) is to promote the use of electronic health records to improve the efficiency and quality of the healthcare system through enhanced information sharing. HIPAA focuses on protecting the security (including availability, integrity, and confidentiality) and privacy of Protected Health Information (PHI) during creation, receipt, maintenance, and transmission by covered entities and their business associates.

	Entities subject to HIPAA are required to implement appropriate security measures when processing, maintaining, and storing PHI. Tencent Cloud conducts self-assessments to ensure its capability to protect personal information and the effectiveness of its control measures in compliance with HIPAA requirements.
SEC Rule 17a-4 [US]	Tencent Cloud Object Storage (COS) has been certified by an independent third-party assessment firm specializing in records management and information governance, based on the technical requirements of the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Commodity Futures Trading Commission (CFTC). This certification provides assurance for customers operating in highly regulated environments, such as the financial services industry, regarding the non-rewriteable, non-erasable preservation method and object lock feature of Tencent COS, demonstrating Tencent Cloud's commitment to delivering secure and industry-compliant cloud products.
The center for Financial Industry Information Systems (FISC) [Japan]	To enhance the security of financial institutions, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions provide effective guidance for Japanese banks and financial institutions in building secure information systems and ensuring their stable operation. Tencent Cloud has assessed its control measures against these guidelines to confirm that relevant measures meet the requirements of the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions.
BS10012: 2017 [UK]	BS10012:2017 was published by the British Standards Institution to provide organizations with a compliance framework and good practices for privacy protection. It guides businesses in establishing and maintaining a Personal Information Management System (PIMS) to ensure adequate and appropriate controls for protecting personal information. The standard has been updated and revised to align with the General Data Protection Regulation (GDPR). Tencent Cloud has obtained BS10012:2017 certification, demonstrating that its personal information management system meets international standards and industry best practices, enabling customers to better comply with GDPR privacy protection requirements.
CISPE Code of Conduct [EU]	The CISPE Code of Conduct is a pan-European, sector-specific code for cloud infrastructure service providers under Article 40 of the EU General Data Protection Regulation (GDPR). It helps organizations across Europe accelerate the development of GDPR compliant cloud-based services for consumers, businesses, and institutions. Tencent Cloud has awarded "Candidate" mark of CISPE Code of Conduct, which means the cloud service provider has fulfilled the self-assessment against the CISPE Code of Conduct requirements.
NIST CSF Certification	NIST CSF is a framework that focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risk as part of an organization's risk management process. It helps organizations adjust and prioritize their cybersecurity activities based on business needs, risk tolerance, and resources, and improve security and resilience by applying the framework's risk management principles and guidelines. Tencent Cloud has obtained NIST CSF certification from an independent third-party organization, which affirms the capability of its cybersecurity defense system and demonstrates its ability to effectively identify, resist, respond to,

	and manage security risks, protecting cloud assets and data and enhancing confidence in security and stability.
PCI DSS Certification	The Payment Card Industry Data Security Standard (PCI DSS) is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC). To enhance the security of cardholder data, PCI DSS provides a globally unified benchmark for technical and operational requirements to protect account data. It applies to all entities involved in payment card processing, such as merchants, processors, acquiring institutions, issuing institutions, service providers, and other entities that store, process, or transmit cardholder data. Tencent Cloud has passed PCI DSS certification and obtained Grade 1 Service Provider qualification, demonstrating its capability to provide secure and reliable payment services and protect cardholder data.
GxP compliance	In the healthcare industry, GxP refers to a set of regulations, guidelines, or industry best practices that govern compliance-related activities for medical products such as pharmaceuticals, medical devices, and medical software applications. Tencent Cloud has published a GxP compliance white paper to explain how its management processes and technical measures help customers meet the requirements of GxP computerized systems and ensure the confidentiality, integrity, and availability of business data hosted on Tencent Cloud.

03 Tencent Cloud Security Responsibility Sharing Model



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

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

	IaaS	PaaS	SaaS	
Customer Responsibilities	Cloud Customer Data Security	Cloud Customer Data Security	Cloud Customer Data Security	
	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.

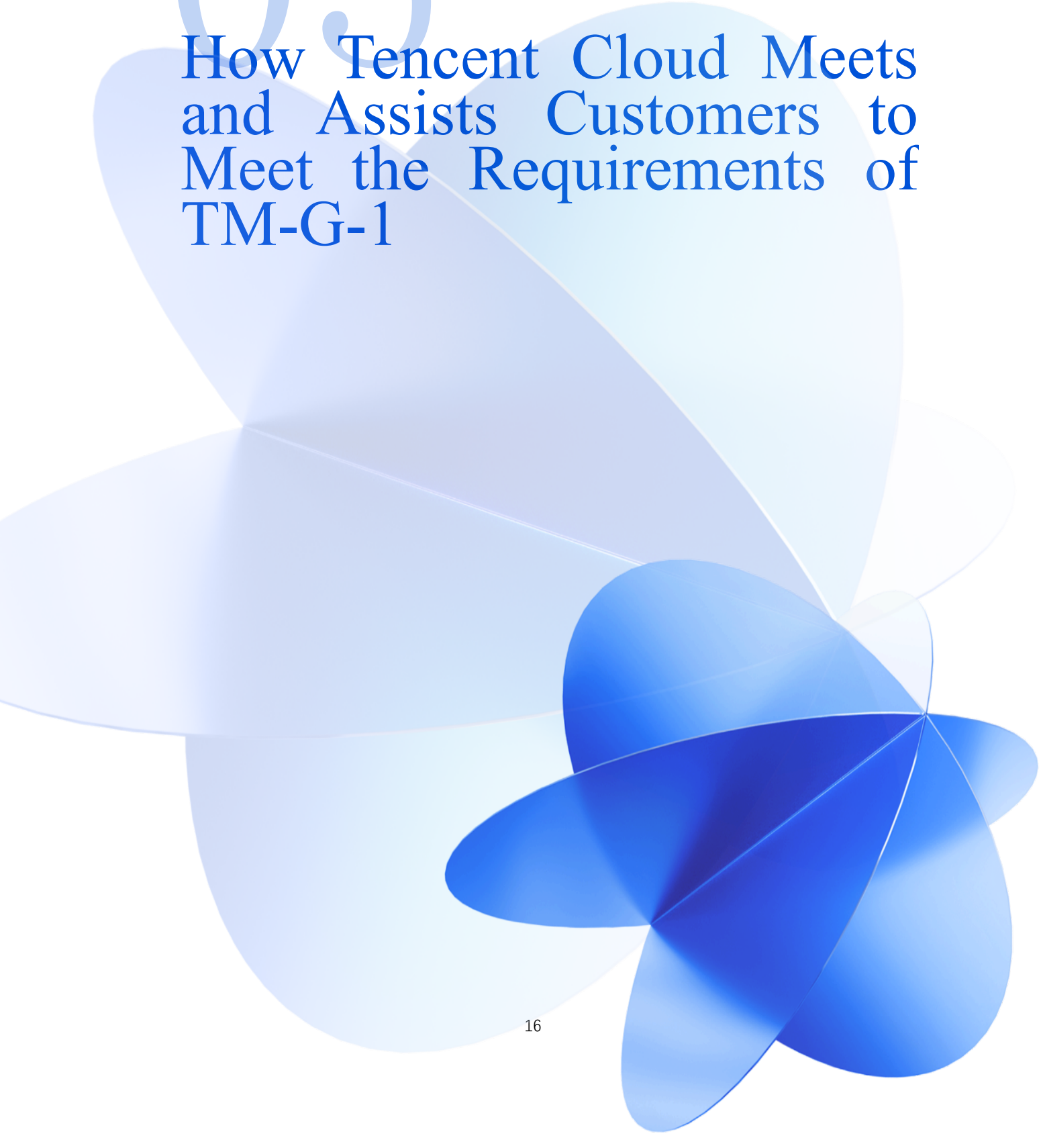
- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically 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 TM-G-1



TM-G-1 General principles for technology risk management provides guidance to Authorized Institutions on general principles to consider when managing technology-related risks. The requirements primarily cover areas such as IT governance, security management, system development and change management, information processing, communication networks, and management of technology service providers.

In this section, Tencent Cloud summarizes the control requirements in TM-G-1 that are relevant to cloud service providers, and explains how Tencent Cloud, as a cloud service provider, supports Authorized Institutions in complying with these regulatory expectations.

5.1 IT Control Governance

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.1	IT Control Governance	2.1.1 The senior management of AIs should establish a set of IT control policies that define the fundamental rules for IT governance. 2.1.2 These policies should be reviewed regularly and updated as necessary to reflect changes in the operating environment and technological developments. 2.1.3 Senior management should ensure that clear procedures are in place to verify compliance with IT control policies, as well as procedures for approving any exemptions from these policies. 2.1.4 Senior management may implement appropriate mechanisms to periodically remind relevant staff of the IT control policies.	Customers should establish a set of IT control policies, review and update these policies regularly, develop procedures to verify compliance with IT control policies, and implement appropriate mechanisms to remind employees of policy issuance and updates. To support customers in meeting regulatory requirements, Tencent Cloud has formulated an information security management policy, which consists of an overall security strategy, security organizational structure, and security management system. This effectively supports the security and risk management of the cloud platform and guides the daily work and management processes of all departments and employees. Tencent Cloud's information security policies are reviewed annually to ensure that the objectives, procedures, and measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, and to confirm the adequacy and effectiveness of the information security policies. Employees can access these policies through Tencent Cloud's internal platform. In addition, Tencent Cloud incorporates information security management into daily operations and provides regular information security training to employees to ensure they understand and comply with internal information security management policies and requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
2.5	Staff competence and training	2.5.1 Senior management should ensure that staff of IT, technology risk management, and internal technology audit functions possess appropriate capabilities and continuously meet the required levels of professional knowledge and experience. At the same time, staffing levels should be sufficient to handle current and anticipated workloads. 2.5.2 AIs must establish appropriate procedures to identify whether staff responsible for technology-related functions have any significant technical gaps.	Customers should ensure that employees in IT and related departments possess the capabilities, professional knowledge, and experience required for their roles, and that staffing levels match current and anticipated workloads. To support customers in meeting regulatory requirements, Tencent has established a Security Technology Committee and professional security teams across different functions and areas. Tencent has also implemented comprehensive internal human resource management standards and procedures to ensure recruitment and staffing are aligned with job requirements. During the recruitment process, Tencent Cloud conducts background checks on prospective employees, including verification of academic qualifications and certifications. Tencent Cloud has also established an information security training mechanism, requiring formal employees, consultants, interns, and outsourced personnel to complete information security training courses. Tencent Cloud offers a variety of training programs, including mandatory courses for all employees, specialized training for key positions, and elective professional courses. Training content covers areas such as basic security awareness, office security, vulnerability identification and defense, privacy protection, incident response, secure development practices, and data security requirements.

5.2 Protection

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.1	Information classification and protection	3.1.3 Regardless of the media used to store information, AIs should establish measures to ensure information confidentiality, ensure that all media are adequately protected, and set up secure processes for the disposal and	Customers should implement effective confidentiality and protection measures for all media storing information, adopt industry-recognized encryption solutions and key management practices, and establish processes for the disposal and destruction of sensitive information stored on media. **To ensure the confidentiality and integrity of**

No.	Domain	Summary of Controls	Tencent Cloud's Response
		destruction of sensitive information stored on paper and electronic media. 3.1.4 If encryption technology is used to protect the confidentiality and integrity of AIs' information, AIs should adopt industry-recognized encryption solutions and implement sound key management practices to safeguard the relevant cryptographic key	**customer data during storage and meet regulatory requirements**, multiple Tencent Cloud products such as **TDSQL-C (cloud-native database)**, **MySQL**, and **Object Storage (COS)** support data encryption using secure, high-strength encryption algorithms. These products integrate with the **Key Management Service (KMS)** to enable full lifecycle management of encryption keys and ensure data confidentiality. **KMS** uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect keys, employs secure data transmission protocols, and supports key lifecycle management. To reduce the risk of key compromise or misuse, KMS supports key rotation and adopts secure and reliable methods to delete expired, invalid, or compromised keys. Deleted keys cannot be recovered, and data encrypted under those keys cannot be decrypted. **For the disposal and destruction of sensitive information**, Tencent Cloud provides secure and reliable data destruction mechanisms. When a customer's cloud service is terminated, Tencent Cloud follows strict data erasure procedures, ensuring that all customer data, including copies and backups, is permanently deleted after the retention period expires and cannot be restored. When media used to provide Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud follows strict processes for complete physical destruction. **Regarding Tencent Cloud's internal use of encryption algorithms and key management,** Tencent Cloud has established security management standards specifying requirements for key application, generation, storage, usage, transmission, update, and destruction. All operations involving the key lifecycle follow basic requirements such as dual control, secure handover, proper custody, and timely updates. During key usage, Tencent Cloud enforces separation of duties, strict approval, and real-name operations, and retains business key operation logs

No.	Domain	Summary of Controls	Tencent Cloud's Response
			for regular audits. For encryption during data transmission and storage, Tencent Cloud requires internal teams to comply with international cryptographic standards and regulations, use high-security algorithms such as AES-256, and ensure key lengths meet security requirements.
3.2	Authentication and access control	3.2.1 Access to information and application systems should be restricted by appropriate authentication mechanisms and supported by access control rules. Each application system should identify all users through unique user identification codes and appropriate authentication methods to ensure accountability for their activities. 3.2.2 AIs should establish effective password rules to ensure that easily guessed passwords are not used and that passwords are changed regularly. Stronger authentication methods should be adopted for higher-risk transactions or activities.	Customers should use appropriate authentication mechanisms to control access to application systems and data and establish effective password policies. Cloud Access Management (CAM) helps customers securely and precisely 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, users can modify password policies for sub-users, including complexity, length, and validity period. To prevent password leakage, Tencent Cloud applies SHA256 hash encryption and salting to customer passwords, avoiding storage of passwords in plain text. CAM also supports multiple methods of secondary identity verification to confirm identity and environment security before login and sensitive operations. When customers create CAM sub-users and grant permissions, employees can log in to the Tencent Cloud console using sub-user credentials or access resources under the primary account via cloud APIs using sub-user keys. To support customers in meeting regulatory requirements, Tencent Cloud has also established internal access control management standards, requiring user accounts to use unique identifiers and setting password policies for employee accounts based on security baselines, including password length, complexity, lockout, and reset rules. In addition, Tencent Cloud uses a zero-trust security management system for employee access authentication, requiring two-factor authentication

No.	Domain	Summary of Controls	Tencent Cloud's Response
			before accessing internal resources.
3.2	Authentication and access control	3.2.3 Extra care should be exercised when controlling the use of and access to privileged and emergency IDs. AIs must establish control measures including approval mechanisms, monitoring mechanisms, and safeguarding measures for privileged and emergency IDs.	Customers should implement controls over privileged and emergency accounts, including safeguarding, approval, usage logging, and monitoring of such accounts. **Cloud Access Management (CAM)** provides fine-grained permission control to help customers manage privileged and emergency accounts by granting specific permissions to different personnel for different resources. Customers can also use **CloudAudit** to view and track employee operation records. CloudAudit supports online viewing of Tencent Cloud console and cloud API operation logs for up to 90 days. Tencent Cloud has defined management requirements and authorization mechanisms for special access privileges. Bastion Hosts are fully deployed across Tencent Cloud's production environment to centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain authorization approval before accessing the Bastion Host, and only designated Tencent Cloud staff are permitted to log in. Bastion Host login requires two-factor authentication. Operation records are centrally stored on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these logs.
3.3	Security administration and monitoring	3.3.1 A security administration function and formal procedures should be established to manage the allocation of access rights to system resources and application systems, and to monitor the use of system resources to detect any unusual or unauthorized activities.	Customers should manage the allocation of system resources and application system permissions, separate security management responsibilities, and monitor the use of system resources. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		3.3.2 AIs should appropriately segregate duties within the security administration function or implement other compensating controls to reduce the risk of unauthorized activities being performed by the security administration function.	operation records through **CloudAudit**. In addition, Tencent Cloud provides **Bastion Host (BH)**, which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Tencent Cloud has established authorization policies and a permission segregation matrix for access control. Permissions are assigned based on job responsibilities, with effective time limits set for these permissions, enabling fine-grained control over access rights. Tencent Cloud maintains records of personnel identity information corresponding to job roles and permission levels for each business system and conducts regular internal permission reviews to prevent misuse or abuse of permissions. Tencent Cloud has also set detailed operational security "red lines" and leveraging years of experience in abnormal behavior monitoring, has built a comprehensive rule base and developed reliable automated auditing tools for operational security to promptly identify abnormal behaviors and trigger real-time alerts.
3.3	Security administration and monitoring	3.3.3 AIs should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours, including timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches.	Customers should establish incident response and notification procedures to handle and report information security incidents in a timely manner. To support customers in meeting regulatory requirements, Tencent Cloud has developed an information security incident management standard and established mechanisms for incident response and handling. Tencent Cloud uses an internal security operations system to record security incidents. For detected and identified security incidents, Tencent Cloud analyzes and classifies them based on factors such as the nature of the incident, data sensitivity, and scope of impact, and promptly informs the personnel

No.	Domain	Summary of Controls	Tencent Cloud's Response
			responsible to follow up and address the incident. **For communication and notification**, Tencent Cloud has defined procedures for incident response, escalation, and notification to ensure timely alerts or notifications to internal staff, customers, and other relevant parties who may be or have been affected by the incident. This ensures that all parties can communicate and coordinate in an orderly, timely, and efficient manner. **For security incidents that may affect customers**, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels and provide technical support to help customers take remedial measures to minimize losses. For more information on incident response and notification, please refer to Section 11: How Tencent Cloud complies with and assists customers in meeting the "Incident Response and Management Procedures.
3.4	System security	3.4.1 AIs should establish control procedures and baseline security requirements to safeguard application programs, operating systems, system software, and databases, such as: • appropriate methods for identifying and authenticating user identities, supported by proper authorization arrangements; • periodic checks on the integrity of static data (e.g., system parameters); • secure configuration of operating systems, system software, databases, and servers;	Customers should establish control procedures and security baselines for applications, operating systems, system software, and databases. These should include identity authentication and access control, static data integrity checks, secure configuration and configuration records, patching and updates, as well as logging and monitoring of system and user activities. To assist customers in meeting regulatory requirements, Tencent Cloud provides a range of services to support security baseline configuration and system protection, such as: • **Cloud Access Management (CAM)**: Offers secure and fine-grained user and permission management. • **Cloud Security Center (CSC)**: A one-stop security management platform that provides automated risk assessment of cloud product configurations, covering services such as CVM, COS, cloud databases, and CLB,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		• timely identification, assessment, testing, and application of necessary patches and security updates developed by vendors; • proper documentation of all configurations and settings of operating systems, system software, databases, and servers in plain text, with regular verification of security settings; • adequate logging and monitoring of system and user activities, with secure retention of related records.	helping customers reduce risks caused by misconfigurations. • **Cloud Workload Protection Platform (CWPP)**: Leverages Tencent's extensive threat intelligence to help customers manage baseline security. It provides default baseline policies, baseline inspection capabilities, and supports compliance rate queries and remediation recommendations. • **Configuration Audit (Config):** Enables centralized auditing and governance of cloud resources, continuously recording configuration details and changes across regions. It automatically evaluates compliance based on Tencent Cloud best practices and compliance templates, identifying non-compliant configurations for automated monitoring and management. • **Cloud Log Service (CLS)**: Helps customers address operational, security monitoring, log auditing, and analysis needs. CLS uses a highly available distributed architecture with redundant backups to ensure stable and reliable log data services. • **CloudAudit**: Supports regulatory compliance checks, operation reviews, and risk audits for Tencent Cloud accounts. Cloud Audit allows online viewing of console and API operation records within the past 90 days. • **Elasticsearch Service (ES)**: Aggregates real-time logs from CVM, containers, and other cloud products, as well as business data, into Tencent Cloud ES clusters for distributed storage, search, and analysis. To further support customers in meeting regulatory security requirements for applications, operating systems, system software, and databases, Tencent Cloud has also established a comprehensive internal security management framework:

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• Tencent Cloud has defined internal account application and deactivation processes, as well as access control requirements for operating and application systems. Bastion hosts are deployed in production environments to centrally manage administrator account permissions for backend components. • Tencent Cloud has developed standardized security configurations for network devices, firewalls, servers, databases, and applications, and regularly reviews baseline content. Internal monitoring systems track routers, firewalls, and servers, while Endpoint Detection and Response (EDR) tools provide full asset control. EDR supports antivirus, intrusion detection, baseline and vulnerability scanning, and compliance auditing of commands and login activities, triggering alerts for malicious programs or abnormal behaviors. Patch installation status is continuously scanned, and overdue patches are recorded via work orders. • Internal operations strictly control change activities, ensuring proper approval and testing before production deployment, and preventing unauthorized parameter changes. • Tencent Cloud enforces detailed operational security "red lines" and uses AI-driven automated auditing tools powered by credit, behavior, and content engines to detect anomalies and trigger real-time alerts.
3.5	End-user and mobile computing	3.5.3 AIs should establish procedures and responsibilities to detect and prevent attacks by computer viruses and other malicious software on software and information processing facilities. For example: • prohibiting the download and use of unauthorized files and software, and access to suspicious	Customers should establish procedures and implement controls to detect and prevent computer viruses or other malicious software attacks targeting software and information processing facilities. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		websites; • installing anti-virus software provided by trusted vendors; • prohibiting the download of executable files and mobile code; • performing timely and regular virus scans on all computing devices and mobile users' computers.	prevention, abnormal login alerts, Trojan file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by servers. **To help customers meet regulatory requirements for server virus protection**, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage all server endpoints. 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. **For personal computer usage management**, Tencent Cloud has established software security standards that define restrictions on software usage on personal computers (including laptops and workstations). Application whitelisting technology is used to allow only known and trusted programs to run, reducing the risk of malware intrusion. Tencent Cloud also uses a Zero Trust Security Management System to manage personal computer endpoints, providing capabilities such as virus removal, vulnerability remediation, and proactive defense to deliver comprehensive protection against ransomware, phishing attacks, and lateral movement threats.
3.6	Physical and personnel security	3.6.1 AIs should implement physical security measures to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be located in secure areas. Access to secure areas should be restricted to authorized personnel only, and access rights should be reviewed and updated	Customers should implement physical security measures to protect computer facilities and equipment from damage or unauthorized access, while fully considering environmental risks related to data centers. To assist customers in meeting regulatory requirements, Tencent Cloud has established a physical security management framework to standardize operational safety, promptly identify risks, and strengthen physical security controls. **In terms of site selection and environmental safety,** Tencent Cloud's global data centers are

No.	Domain	Summary of Controls	Tencent Cloud's Response
		regularly. 3.6.2 When selecting data center locations, AIs should fully consider environmental risk factors and implement physical and environmental control measures to monitor conditions that may adversely affect the operation of information processing facilities.	selected, constructed, or leased in accordance with relevant international standards and local security requirements. Each data center is equipped with a complete fire protection system, and power and cooling systems adopt highly stable, fully redundant designs to prevent single points of failure. Anti-static flooring is installed throughout the facilities, and grounding wires are applied to racks and cable trays to prevent electrostatic damage to equipment. **In terms of security and monitoring,** Security personnel at Tencent Cloud data centers conduct inspections strictly according to checklists and schedules, signing and recording inspection times at each checkpoint. If infrastructure failures or security incidents are detected, the emergency response process is immediately activated. Data centers are equipped with 24/7 video surveillance systems with no blind spots, monitored from a security control room. Surveillance records are securely stored and retained for an adequate period. Tencent Cloud data centers enforce strict access control policies based on zone security levels. All visitors and staff must undergo identity verification and personal item checks, with detailed registration of carried items.
3.6	Physical and personnel security	3.6.3 To control access by third-party personnel to secure areas, AIs should have formal approval procedures for entry and closely monitor their activities. Appropriate screening procedures should be established for the recruitment of permanent and temporary technical staff and contract employees.	If third-party personnel need to enter an organization's secure areas, customers should establish admission and monitoring mechanisms for such personnel. For both long-term and temporary technical staff or contract employees, customers should conduct appropriate background checks prior to engagement to ensure their qualifications, professional history, and reliability meet job requirements and security standards. **In terms of access management and monitoring in the secure zone,** to assist customers in meeting regulatory requirements, Tencent Cloud has implemented corresponding control measures, including visitor application and approval processes, as well as escort mechanisms. Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Cloud data centers maintain a comprehensive access control security matrix within the authorization system, based on personnel categories and access permissions, to effectively manage access and operational activities. Before third-party personnel can access a Tencent Cloud data center, they must submit valid identification details, visit purpose, time, and designated area for authorization. Access is granted only after approval, and the entire visit must be accompanied by Tencent Cloud staff. **In terms of personnel recruitment and management,** Tencent Cloud's HR department conducts background checks on new employees and updates them as needed. Additionally, Tencent Cloud ensures the security of its IT control environment for technology service providers through strict vendor security assessments, regular monitoring and annual evaluations, independent audits, and clearly defined outsourcing agreements.

5.3 System Development and Change Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.2	Project life cycle	4.2.1 AIs should adopt and implement a complete project life cycle methodology to manage the development, implementation, and maintenance of major computer systems. 4.2.2 The project life cycle methodology should clearly define the roles and responsibilities of the project team and the deliverables for each phase. It should also include a process to ensure that appropriate security requirements are identified	Customers should establish and implement a comprehensive project lifecycle management methodology to define processes for critical system development, testing, acceptance, implementation, and operations. This includes identifying, developing, testing, and enforcing security requirements, as well as conducting quality reviews for major technology-related projects. To support customers in managing the development lifecycle, Tencent Cloud provides **Cloud Native Build (CNB)** developer tools. CNB is based on the Docker ecosystem and abstracts environments, caches, and plugins using declarative syntax, enabling developers to build software more efficiently. CNB offers a complete developer toolchain with capabilities such as code hosting,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		when formulating business requirements and incorporated during development, testing, and implementation. 4.2.3 An independent party not involved in project development should conduct quality assurance reviews of major technology-related projects when necessary. 4.2.4 A formal acceptance process should be established to ensure that only systems that have been properly tested and approved are promoted to the production environment. Acceptance testing should be carried out in an environment separated from the production environment. Production data should not be used for development or acceptance testing unless the data has been desensitised and prior approval from the information owner has been obtained. Newly developed systems should also undergo performance testing before being promoted to the production environment.	high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and custom task sets, effectively supporting the entire process from requirements to deployment and enabling agile development management. Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls throughout the product lifecycle. Key security measures include: • Security Training: Developers receive secure coding training and are required to follow secure coding guidelines. • Requirements Analysis: Engage in discussions on business content, workflows, and technical frameworks to identify optimal security integration points. • System Design: Perform threat modeling and security assessments of the chosen architecture. • System Development: Provide Tencent-designed secure development components and enforce secure coding practices. • Security Validation: Conduct code security checks, asset scans, web vulnerability scans, manual security assessments, penetration testing, and code audits to identify vulnerabilities. • Release: Systems are deployed to production only after all high-risk issues have been fixed to prevent vulnerabilities from entering the live environment. Tencent Cloud ensures that the development/testing environment and the production environment are isolated from each other, and prohibits the use of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			unsensitized production data in the development/testing environment.
4.3	Change management	4.3.1 AIs should establish formal change management procedures, which should include: • classification and prioritization of changes, and determination of change impact; • roles and responsibilities of relevant parties, with adequate segregation of duties; • program version control and audit trails; • scheduling, tracking, monitoring, and implementation of changes to minimize business disruption; • rollback processes to restore original programs, system configurations, or data in case of production release issues; • post-implementation verification of changes made. 4.3.2 AIs should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner and other relevant parties at the time of or immediately after the change. 4.3.3 Emergency changes should be logged and backed up to allow restoration of previous	Customers should establish change management procedures, including impact assessment, approval, implementation, tracking, and rollback. Customers should also define emergency change management procedures, covering approval, documentation, backup, review, implementation, and subsequent remediation. To assist customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive change management standard for product and configuration changes. This standard clearly defines each step of the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also has 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 and rollback planning before deployment and require approval from designated responsible personnel. Tencent Cloud's change release system enforces strict controls, allowing only authorized personnel to execute change operations and retaining detailed change logs for regular audits. After deployment, Tencent Cloud operations team verifies and monitors changes in the production environment and records the results. For operational changes that may affect customers, Tencent Cloud promptly issues change notifications through official channels such as the website and internal messaging.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		program versions and data files if necessary. Emergency changes should be reviewed by independent personnel and subsequently replaced by proper fixes through formal acceptance testing and change management procedures.	

5.4 Information Processing

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.1	IT operations management and support	5.1.2 Detailed operational instructions such as computer operator tasks, job scheduling and execution should be documented in an IT operations manual. The IT operations manual should also include the procedures and requirements for on-site and off-site backup of data and software in both production and development environments.	Customers should develop an IT operations manual that clearly documents detailed operating instructions for technical personnel, work schedules, and backup requirements for data and software in both production and development environments. To help customers ensure operational security, Tencent Cloud has established operations management standards that provide clear guidelines and requirements for routine maintenance activities. Tencent Cloud uses mature, automated operations management platforms to manage operational tasks and strictly controls changing windows through internal mechanisms, ensuring that all requests are completed within designated timeframes. Tencent Cloud also enforces detailed operational security "red lines" and conducts regular internal security reviews. To ensure that operations within the production environment are controlled and traceable, all backend maintenance activities are thoroughly logged and centrally stored on the log platform. Tencent Cloud's internal audit team regularly reviews these logs to identify and investigate suspicious activities during operations.
5.1	IT operations management and support	5.1.3 AIs should establish an incident management system to enable prompt response to IT operational incidents, report incidents to relevant IT	Customers should establish an incident and problem management mechanism to ensure rapid response, reporting, documentation, analysis, and tracking of IT operational incidents until resolution. A help desk should also be set up to provide first-line support for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management personnel, and record, analyze, and track all incidents until they are resolved. AIs may set up a central help desk to provide frontline support to users for all technology-related incidents and refer incidents to the appropriate departments for investigation and resolution.	user technical issues. To assist customers in responding quickly to technical incidents, Tencent Cloud offers comprehensive operational security capabilities and 24/7 technical support. Tencent Cloud provides multiple support channels, including 24/7 ticketing, 24/7 hotline, intelligent customer service, and self-service options, ensuring uninterrupted handling of customer inquiries and feedback. The customer service team and technical experts deliver prompt and effective assistance, helping customers efficiently identify root causes, track incident progress, and provide suitable solutions. Beyond basic support services, enterprise customers with complex business systems can opt for tailored service plans, which include dedicated support groups, a designated technical account manager, and value-added services for enhanced support.
5.2	Performance monitoring and capacity planning	5.2.1 AIs should implement a process to ensure continuous monitoring of application system performance and timely, comprehensive reporting of exceptions. The performance monitoring process should include forecasting capability to identify and correct problems before they affect system performance. This process should assist in preparing workload forecasts to identify trends and provide information required for capacity planning. 5.2.2 Capacity planning should extend beyond the production environment to include backup systems and related facilities.	Customers should establish procedures to continuously monitor application system performance, promptly and comprehensively report anomalies, and identify trends for capacity planning. **Tencent Cloud's Observability Platform (TCOP)** provides real-time monitoring, analysis, and alerting services for cloud products and resources. TCOP collects monitoring metrics reported by cloud services such as CVM and cloud databases, as well as custom metrics defined by customers, and displays them through visual dashboards. This helps customers track resource utilization, application performance, and the operational status of cloud products in real time. TCOP supports setting alerts for specific metrics and notifies customers of business anomalies through message push and other channels based on configured alert rules. Tencent Cloud has also established an internal capacity management process, assigning responsibility to business units for forecasting and planning system capacity. Tencent Cloud uses an internal capacity monitoring platform to track usage trends in real time. Business units leverage historical

No.	Domain	Summary of Controls	Tencent Cloud's Response
			capacity data and consider new business and system requirements to forecast capacity needs and develop annual capacity management plans, ensuring business continuity.
5.3	IT facilities and equipment maintenance	To ensure the continued availability of AIs' technology-related services, AIs should maintain and service IT facilities and equipment in accordance with industry practices and suppliers' recommended service intervals and specifications, and keep appropriate records. A hardware and facility inventory should be maintained to control and track all purchased and leased hardware and software.	Customers should regularly maintain and inspect IT facilities and equipment, keep corresponding records, and maintain a detailed inventory of hardware, infrastructure, and software assets. To help customers comply with regulatory requirements for managing IT facilities and equipment, Tencent Cloud has implemented the following measures: **In terms of asset management,** Tencent Cloud has established an information asset management standard and a full lifecycle management process to classify and protect assets such as electronic data, hardware and virtual devices, infrastructure, application systems, and software. Through its asset management system, Tencent Cloud manages hardware and software components, including asset registration and binding, inventory checks and updates, and asset retirement and replacement, ensuring stable operation of the underlying cloud platform and reliable support for business systems. Tencent Cloud regularly retires and replaces servers, and software components (such as operating systems and database systems) are upgraded to appropriate versions before end-of-support. For decommissioned hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction process. **In terms of infrastructure maintenance and monitoring,** Tencent Cloud assigns on-site data center personnel to regularly inspect critical equipment in server rooms, following predefined procedures to record inspection results, report anomalies, and resolve identified issues promptly to eliminate security risks and ensure stable operation of equipment. Tencent Cloud also deploys monitoring systems to continuously track key

No.	Domain	Summary of Controls	Tencent Cloud's Response
			metrics of critical data center equipment 24/7. In case of anomalies, alerts are automatically sent to on-site personnel.
5.4	Disaster recovery planning	AIs should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. Please refer to TM-G-2 "Business Continuity Planning" on how to develop detailed recovery procedures of application systems and technology services and ensure adequate insurance coverage of IT resources.	Customers should establish a disaster recovery plan to ensure that critical application systems and technology services can be restored in accordance with business recovery requirements. **To support customers in developing disaster recovery plans**, Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse needs such as multi-redundant backups and cross-region disaster recovery. Additionally, to ensure rapid response and restoration of critical functions following a cybersecurity incident, Tencent Cloud provides highly available cloud products and services, including compute, networking, storage, databases, containers, middleware, and security services. Tencent Cloud has developed detailed disaster recovery plans for cloud products and key processes and conducts regular drills to ensure timeliness and feasibility. Tencent Cloud has established a comprehensive business continuity and disaster recovery management system, certified to the ISO/IEC 22301 Business Continuity Management System international standard. For more details on business continuity and disaster recovery, please refer to Section 6: How Tencent Cloud Complies with and Assists Customers in Meeting TM-G-2 Business Continuity Planning.

5.5 Communications Networks

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.1	Network management	6.1.1 Protecting communications networks requires robust network design, clearly defined network services, and adherence to sound discipline in network	Customers should protect communication networks through robust network design, clearly defined network services, sound network management practices, and continuous monitoring. Network management responsibilities should be clearly assigned, and network designs, standards, diagrams,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management. 6.1.2 AIs should clearly assign overall responsibility for network management to designated personnel who possess appropriate knowledge, skills, and resources to perform their duties. Network standards, design, diagrams, and operating procedures should be formally documented, updated as necessary, communicated to all relevant network staff, and reviewed periodically. 6.1.3 AIs should identify communications facilities that are critical to the continuity of network services and establish alternate routes to reduce single points of failure. 6.1.4 AIs should continuously monitor the network to reduce the likelihood of network traffic overload and detect network intrusions. 6.1.5 Powerful network analysis and monitoring tools should be protected against unauthorized use. Such tools should be strictly limited to authorized personnel and subject to stringent approval and review procedures.	and operating procedures should be documented. Critical communication facilities supporting network service continuity should be identified and equipped with backup paths, and the use of network analysis and monitoring tools should be restricted and safeguarded. **To ensure network resilience**, Tencent Cloud operates data centers across multiple global regions. Each availability zone connects to multiple carriers at its network egress points, building cross-region disaster recovery capabilities and reducing the impact of carrier-level public network failures. Tencent Cloud's core network adopts a redundant architecture, combined with routing-level path prioritization and traffic engineering to maintain service continuity and prevent single-point failures. **Tencent Cloud also provides customers with multiple services for effective network security management:** • Virtual Private Cloud (VPC): Uses tunneling technology to create virtual networks on physical infrastructure, achieving complete logical isolation between VPCs. Security groups and network ACL rules enable granular control of inbound and outbound traffic at both instance and subnet levels. • Cloud Firewall (CFW): Offers ACL-based firewall control, IPS real-time interception, virtual patching, and malicious code detection to protect network boundaries. • Web Application Firewall (WAF): Defends against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and malicious crawlers. • Anti-DDoS: Combines abundant, high-quality DDoS mitigation resources with evolving proprietary and AI-driven detection algorithms to counter DDoS attacks. • Flow Logs (FL): Provides real-time, non-

No.	Domain	Summary of Controls	Tencent Cloud's Response
			intrusive traffic collection, storage, and analysis to support troubleshooting, architecture optimization, security detection, and compliance auditing. Tencent Cloud has established a network security management standard and a layered defense system. Through policies and processes, Tencent Cloud defines security controls, protection standards, and corresponding roles and responsibilities to ensure secure network operations. Tencent Cloud deploys a mature security architecture incorporating firewalls, IDS/IPS, DDoS protection, network isolation, and web security mechanisms to detect, filter, and block malicious traffic. Internal monitoring systems continuously track routers, firewalls, and network servers, issuing alerts when anomalies occur. Access to internal network resources, including network analysis and monitoring tools, is strictly controlled through permission management and approval workflows to prevent unauthorized access.
6.2	Network security and certification	6.2.1 To prevent insecure connections to an AI's network, AIs should establish and enforce procedures for the use of networks and network services, covering available networks and services, authorization procedures, and controls and procedures to protect access to network access points, network connections, and network services. 6.2.2 AIs should consider segregating internal networks into different segments, taking into account the access control required for the data stored in, or systems connected to, each segment. Sensitive data exchanges between different network segments should be properly controlled and	Customers should establish and enforce procedures for using networks and network services to prevent insecure connections and regularly monitor network device security parameters and audit logs to ensure that network operators receive timely alerts about potential security issues. Additionally, accredited organizations should segment internal networks and implement appropriate controls and safeguards for sensitive data exchanges between different network zones. **In terms of network communication security,** all communications on the Tencent Cloud Console are encrypted using the HTTPS protocol. Tencent Cloud's cloud API interfaces provide HTTPS encryption, signature verification, and status monitoring to ensure port-level communication security for customer operations. **Direct Connect (DC)** offers dedicated, high-security, high-bandwidth network connections, enabling customers to use exclusive network links and reduce data leakage risks. Customers can also use **Cloud Connect Network (CCN)** to establish secure

No.	Domain	Summary of Controls	Tencent Cloud's Response
		protected. 6.2.3 Security parameter settings of network devices such as routers, firewalls, and network servers should be reviewed regularly. Audit trails of daily activities on critical network devices should be maintained and reviewed periodically. Network operations personnel should receive timely alerts related to potential security issues.	private interconnections between VPCs or between VPCs and on-premises data centers (IDCs). **In response to the requirements for network partitioning,** Customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources, with customizable IP ranges and routing policies. VPC uses tunneling technology to build virtual networks on physical infrastructure, achieving complete logical isolation between private networks. Within a VPC, customers can configure security groups and network ACL rules to control inbound and outbound traffic at both instance and subnet levels, enabling multi-layered network access control. **To implement network boundary protection**, Tencent Cloud provides the EdgeOne (EO) platform, which leverages Tencent's global edge nodes to deliver security and acceleration services, including DDoS protection, intelligent web defense, bot/crawler attack mitigation, and DNS resolution. EO also supports custom access control rules based on business needs. Customers can further enhance perimeter security using Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services. Cloud Firewall (CFW) offers ACL-based firewall control, IPS real-time interception, virtual patching, and malicious code detection, enabling granular isolation between VPCs and protecting core assets. Web Application Firewall (WAF) defends against web attacks, intrusions, vulnerability exploits, website tampering, backdoors, and malicious crawlers. Anti-DDoS combines abundant mitigation resources with AI-driven traffic cleansing algorithms to counter evolving DDoS threats. **For multi-tenant isolation,** Tencent Cloud enforces strict isolation through virtualization layer access control policies, internal VPC isolation strategies, console permission management and authentication, and secure API session IDs and access keys, ensuring that each user can only access their

No.	Domain	Summary of Controls	Tencent Cloud's Response
			purchased resources. **In terms of network device security**, to meet regulatory requirements, Tencent Cloud has established network security configuration and baseline standards for devices such as routers, firewalls, servers, databases, and applications. Tencent Cloud team regularly reviews security policies and parameter settings for network devices to ensure effectiveness. Internal monitoring systems continuously track network equipment and issue alerts for anomalies, while identified issues are managed and resolved through a ticketing system.

5.6 Management of Technology Service Providers

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.1	Management of technology outsourcing	When managing technology outsourcing, AIs should, in addition to following the general guidance set out in SA-2 "Outsourcing", consider adopting the following control measures: • Technology service providers should have sufficient resources and expertise to comply with the substance of AIs' IT control policies. • The outsourcing agreement should clearly specify the performance standards and other obligations of the technology service provider, as well as matters relating to software and hardware ownership. AIs should consider including provisions requiring the technology service provider to notify or obtain	Customers should implement control measures for managing technology outsourcing, including the selection and evaluation of service providers, outsourcing agreements, responsibilities and rights of both parties, and subcontracting restrictions. **Tencent Cloud designs and operates its cloud services in accordance with internationally recognized information security and IT governance standards and has obtained multiple global security and compliance certifications.** These certifications ensure that Tencent Cloud products and services are validated by independent, accredited third-party organizations. As a cloud service provider, Tencent Cloud actively supports customers' outsourcing management requirements, including providing and signing relevant service agreements based on customer needs and cooperating with customer-initiated audits or assessments. **Regarding subcontracting**, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		approval before subcontracting significant portions of the services, and the original provider should remain responsible for the subcontracted services. • AIs should conduct an annual assessment to ensure that critical technology service providers maintain an adequate IT control environment.	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. For more details on outsourcing, please refer to Section 7 : How Tencent Cloud Complies with and Assists Customers in Meeting SA-2 Outsourcing and Cloud Computing Guidelines.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2

TM-G-2 Business Continuity Planning outlines the Hong Kong Monetary Authority's supervisory approach to business continuity planning and its expectations for sound practices by authorized institutions. The requirements primarily focus on business impact analysis and recovery strategies, development of business continuity plans, backup sites for business and technology recovery, and implementation of business continuity measures.

For business continuity management, Tencent Cloud has designed and implemented a framework tailored to its cloud computing environment, establishing a comprehensive business continuity management system. Tencent Cloud has formulated business continuity policies and standardized related processes, covering areas such as business impact analysis, continuity planning, emergency response and disaster recovery, drills and testing, and crisis management. Tencent Cloud is certified to the ISO/IEC 22301 Business Continuity Management System international standard.

In this section, Tencent Cloud summarizes the control requirements in TM-G-2 relevant to cloud service providers and explains how Tencent Cloud assists authorized institutions in meeting these requirements. Additionally, for related requirements under the HKMA's OR-2 Operational Resilience guideline—such as business continuity and incident response—please refer to the corresponding sections in this chapter.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.1	Business impact analysis	3.1.1 The objective of the business impact analysis is to identify various risks that pose a threat to continuous business operations and to quantify the impact of disruptions. 3.1.2 The business impact analysis normally comprises two stages. The first stage is to identify critical operations that must be maintained and continued in the event of an incident. The second stage is a time-frame assessment, which aims to determine how quickly the organization needs to resume the identified critical operations, taking into account the tolerance for disruption set by the organization. 3.1.3 Based on the results of the business impact analysis, the business and support functions should be able to define the minimum level of critical operations to be maintained in the	Customers should conduct a business impact analysis to identify critical business functions and risks that threaten business continuity, quantify the impact of disruptions on these functions, and determine recovery time objectives (RTO) and the minimum level of service required during an incident. To assist customers in meeting regulatory requirements, Tencent Cloud performs business impact analysis on its cloud products and services based on internal business continuity management policies. This includes identifying critical business processes, analysing potential threats to Tencent Cloud operations, defining recovery time objectives and minimum service levels, and developing appropriate response strategies based on the analysis results.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		event of an incident.	
3.2	Recovery strategy formulation	3.2.1 Business and support functions should formulate their own recovery strategies on how to achieve the minimum level of critical operations and the recovery timeframe established by the business impact analysis. This includes determining an alternate site, the total number of personnel responsible for recovery, as well as the workspace, applications and technology requirements, office facilities, and vital records necessary to provide the required level of operations. 3.2.2 The result of the time-frame assessment in the business impact analysis is the primary factor in determining the recovery priority of individual services. The inter-dependency among critical operations is another major consideration in deciding recovery strategies and priorities.	Customers' critical business units and supporting departments should develop recovery strategies based on recovery time objectives (RTO) and minimum service levels identified in the business impact analysis. To ensure continuous availability of customer operations, Tencent Cloud formulates response strategies and business continuity plans based on the business impact analysis of its cloud products and services. Tencent Cloud has developed detailed disaster recovery plans for cloud products and key processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Regular drills are conducted in strict accordance with requirements to ensure the feasibility and effectiveness of these plans.
4.2	Crisis management process	4.2.2 Senior management should identify potential crisis scenarios and, where applicable, develop relevant crisis management procedures to address these situations. The overall crisis management process should, at a minimum, include the following: • Procedures to ensure early detection of emergencies or disasters and prompt notification of the crisis management team; • Procedures to establish roles and responsibilities for	Customers should establish crisis management procedures to help contain and mitigate the escalation of emergency incidents. These procedures should include incident detection and reporting, impact assessment, conditions for activating the business continuity plan, and internal and external communication protocols. To assist customers in meeting regulatory requirements, Tencent Cloud has developed a crisis management framework that defines processes and responsible teams for handling unexpected or disaster events affecting Tencent Cloud products or services. This framework covers crisis prevention, analysis and response, recovery, and post-crisis

No.	Domain	Summary of Controls	Tencent Cloud's Response
		managing operational disruptions; • Procedures for the crisis management team to assess the overall impact on the organization and to make quick decisions on appropriate response actions; • Arrangements for safe evacuation from business premises; • Internal decision-making process and criteria for activating the business continuity plan and/or alternate sites; • Procedures for gathering up-to-date information for the crisis management team; • Internal and external communication procedures; • Procedures for monitoring the recovery and restoration of affected facilities and business services.	improvement. Tencent Cloud's business continuity management procedures also include emergency incident response and notification workflows, business continuity plan activation steps, recovery processes, emergency site arrangements, and communication strategies for both internal and external stakeholders.
4.4	Business resumption	4.4.2 AIs should pay attention to the resilience of critical technology equipment and facilities, such as Uninterruptible Power Supply (UPS) and cooling systems. These equipment and facilities should be subject to continuous monitoring and periodic maintenance and testing. 4.4.3 Appropriate personnel should be assigned responsibility for IT system recovery, and alternate personnel should be designated for key technology recovery staff.	Customers should pay attention to the resilience of critical technology equipment and facilities, continuously monitor and regularly maintain and test relevant devices and infrastructure, and assign appropriate personnel and backup staff to ensure technical recovery. **To enable customers to respond quickly and restore critical functions after a cybersecurity incident**, Tencent Cloud provides multiple storage and database services with built-in backup capabilities, supporting multi-redundant backups and cross-region disaster recovery. Additionally, Tencent Cloud's compute, networking,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			storage, database, container, middleware, and security services are designed for high availability and are supported by detailed disaster recovery plans. **For infrastructure and equipment resilience,** Tencent Cloud's global data centers use highly stable, fully redundant power and cooling systems to prevent single points of failure from affecting service continuity. Security personnel at each data center conduct inspections according to predefined checklists and schedules, signing and recording inspection times at each checkpoint. If infrastructure failures or security incidents are detected, the emergency response process is immediately activated. **To ensure rapid and effective execution of recovery procedures and support timely disaster recovery for customers**, Tencent Cloud has established a comprehensive business continuity management system that defines roles and responsibilities during recovery. For critical skills or positions, Tencent Cloud implements an AB-role backup mechanism and conducts regular emergency drills and training.
4.5	Business continuity models	4.5.1 AIs may adopt different business continuity models to address prolonged disruptions. The traditional model is the "active/back-up" model, which is based on an active operating site with a corresponding alternate site, both used for data processing and business operations. 4.5.2 Some institutions have adopted an emerging "split operations" model. Under this model, the same critical operations are carried out at two or more widely separated active sites,	Customers should select an appropriate business continuity model based on their business environment risks and operational characteristics to address prolonged disruptions. Tencent Cloud operates data centers across multiple global regions, organized into regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		providing mutual back-up support. Each site has the capability to assume part or all of the work of another site for an extended period. 4.5.4 AIs should determine which business continuity model to adopt based on their risk assessment of the business environment and the characteristics of their own operations.	objectives. Tencent Cloud provides **Cloud Load Balancer (CLB)** to enhance the availability of customer applications. CLB offers secure and efficient Layer 4 and Layer 7 traffic distribution services, enabling horizontal scaling of application systems and eliminating single points of failure. CLB uses a clustered deployment architecture that automatically removes faulty instances and selects healthy ones to ensure stable backend operations.
4.6	Vital record management	4.6.2 Copies of vital records should be stored off-site as soon as possible after creation. Back-up vital records must be readily accessible for retrieval. Access to back-up vital records should be adequately controlled to ensure they are reliable for business resumption purposes. For certain critical operations, AIs should consider the need for instantaneous data back-up. There should be clear procedures specifying how and in what priority vital records are to be retrieved or recreated in the event that they are lost, damaged, or destroyed.	Customers should perform offsite backups of critical records to ensure that backups are easily accessible, properly controlled, and include documented procedures for restoring records in case of damage. For certain critical services, authorized institutions should consider real-time data backups. Tencent Cloud currently operates three independent data centers in Hong Kong, each with separate power and network infrastructure, enabling customers to store, process, and back up data locally within Hong Kong. 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• 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 backups and retention of multiple days of backup data for disaster recovery scenarios.
4.7	Public relations and communication strategy	4.7.1 AIs should formulate a formal strategy for communication with key external parties (e.g. regulators, investors, customers, business partners, suppliers, and the media). The strategy should specify the parties that need to be contacted in the event of a disaster. 4.7.2 The business continuity plan should clearly identify the personnel authorized to speak to the media and pre-assign designated staff responsible for external communications. Important conversations with external parties should be properly documented for future reference. Key contact numbers and email addresses of major external parties should be securely maintained and readily accessible.	Customers should establish a communication strategy with external parties, defining which stakeholders need to be contacted during a disaster, maintaining accurate contact information for key external parties, and recording important conversations with them. To support customers' external communication requirements during incidents, Tencent Cloud's business continuity procedures define internal and external communication strategies for disaster scenarios and provide multiple communication channels to promptly publish information that may affect customers. These channels include console announcements, official website updates, in-platform messages, SMS, and email notifications. Tencent Cloud also offers a ticketing system through the official console, enabling customers to report issues related to security, availability, and confidentiality. The ticketing system uses a tiered response mechanism to prioritize tickets and automatically escalates unresolved issues

No.	Domain	Summary of Controls	Tencent Cloud's Response
			to product or technical teams for collaborative handling, ensuring timely response and resolution of customer requests or feedback.
5.1	Alternate sites for business and technology recovery	5.1.2 AIs should review the extent to which key business units are concentrated in the same or adjacent locations, as well as the distance between the alternate site and the primary site. Alternate sites should be sufficiently distanced from the primary site to avoid being affected by the same disaster. 5.1.3 Alternate sites should be readily accessible and available for use within the time frame specified in the business continuity plan. Where continuous operation is required, the alternate site should be pre-installed with workstations, power supply, telephones, ventilation, and sufficient space. AIs should implement appropriate physical access controls in accordance with their security policies.	Customers' backup sites should be easily accessible, available within the timeframes specified in the business continuity plan, pre-equipped with necessary work facilities, and protected by appropriate physical access controls. Backup sites should also be located at a sufficient distance from the primary site to avoid being affected by the same disaster. To assist customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, enabling customers to flexibly deploy data and systems in different regions or availability zones as needed. Tencent Cloud data centers are selected, constructed, or leased in compliance with relevant international standards and local security requirements. Each facility is equipped with highly stable, fully redundant power and cooling systems, comprehensive fire protection systems, and anti-static flooring. Strict infrastructure and environmental access controls are enforced based on zone security levels. All visitors and staff must undergo identity verification, personal item checks, and item registration before entering the data center.
5.2	Alternate sites for technology recovery	5.2.1 Alternate sites for technology recovery (i.e. back-up data centres), which may be separate from the alternate business site, should have sufficient technical equipment (e.g. workstations, servers, printers, etc.) of appropriate model, size and capacity to meet recovery requirements as specified by AIs BCPs. The sites should also have	Customers' backup data centers should have sufficient technical equipment, telecommunications facilities, and pre-installed network connections. The specifications, scale, and capacity of these facilities should meet the recovery requirements defined in the business continuity plan. To assist customers in meeting regulatory requirements, Tencent Cloud data centers are built or leased in compliance with international

No.	Domain	Summary of Controls	Tencent Cloud's Response
		adequate telecommunication (including bandwidth) facilities and pre-installed network connections as specified by their BCPs to handle the expected voice and data traffic volume.	standards and local security requirements. Each availability zone connects to multiple carriers at its network egress points, creating cross-region disaster recovery capabilities and reducing the impact of carrier-level public network failures. Tencent Cloud's core network adopts a redundant architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point failures. Similarly, Tencent Cloud's compute nodes are deployed with redundancy, and faulty nodes are automatically removed in real time by the scheduler, ensuring high availability for customer workloads.
5.3	Alternate sites provided by vendors or other institutions	5.3.2 The contractual terms should include the lead-time and capacity that vendors are committed to deliver in terms of back-up facilities, technical support or hardware. In some cases, a retainer agreement may be advisable to ensure priority service from the vendors in the face of competing demands from other affected users. The vendor should be able to demonstrate its own recoverability including the specification of another recovery site in the event that the contracted site becomes unavailable.	Customers may specify in contracts or agreements the required timeframes and capacity for service providers to deliver backup facilities, technical support, or hardware, as well as priority services in certain situations. Customers should also require service providers to demonstrate their recovery capabilities. Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure requirements. Customers may also negotiate additional requirements to be included in separate agreements. Regarding recovery capabilities, Tencent Cloud has established a comprehensive business continuity management system and is certified to the ISO/IEC 22301 Business Continuity Management System international

No.	Domain	Summary of Controls	Tencent Cloud's Response
			standard. To ensure continuous availability of customer operations, Tencent Cloud has developed detailed disaster recovery plans for cloud products and key processes and conducts regular drills to validate the timeliness and feasibility of these plans, ensuring rapid restoration of services in the event of an incident.
6.1	Testing and rehearsal	6.1.1 AIs should test and validate their business continuity plans against a series of severe but plausible scenarios that incorporate disruptive events and incidents. Testing should verify staff awareness and preparedness and determine the effectiveness of the business continuity plan in practice. 6.1.2 AIs should determine the frequency of testing based on factors such as the potential impact of a disruption, the number of critical operations, and whether there have been significant changes in the operating environment. Senior management should participate in every test and clearly understand the actions they need to take if the plan is activated. Recovery and alternate personnel should also participate in rehearsals to familiarize themselves with their responsibilities. 6.1.3 When developing the test plan, AIs should review all risks and assumptions underlying the business continuity plan to ensure they remain appropriate. The scope of testing should be comprehensive, covering major components of the plan,	Customers should regularly test their business continuity plans; determine testing frequency based on multiple factors, ensure comprehensive coverage, and require participation from primary and backup recovery personnel. Customers should also prepare test plans and reports, and update business continuity plans and recovery strategies as needed. Customers can use **Tencent Cloud Smart Advisor (TSA)** to assist with planning and executing business continuity tests. TSA is a cloud governance platform for multiple ITOM domains, leveraging Tencent Cloud's extensive operational expertise to optimize cloud infrastructure through risk inspections and fault drills. TSA provides fault injection scenarios across IaaS and PaaS layers, along with industry-specific drill templates covering typical use cases such as cross-zone disaster recovery, helping customers quickly adopt proven solutions to improve system availability. To support regulatory compliance, Tencent Cloud's internal business continuity management framework includes regular emergency response and disaster recovery drills and tests. Tencent Cloud develops drill plans based on its business continuity strategy, conducts risk assessments, and implements safeguards to prevent negative impacts on services during drills. Disaster recovery drills often simulate real-world scenarios, including attack-defense exercises and large-scale

No.	Domain	Summary of Controls	Tencent Cloud's Response
		coordination among key parties, and interdependencies with third parties and internal entities. 6.1.4 AIs should prepare formal test documentation, including the test plan, scenarios, procedures, and results, to ensure thorough and effective testing. After completion, a post-test review report should be prepared and formally signed by senior management. If weaknesses or gaps are identified, the plan and recovery strategies should be updated accordingly.	failures, to comprehensively validate resilience, response speed, and recovery capability. After each drill, relevant teams prepare detailed reports, implement corrective actions, and archive documentation for future reference.
6.2	Periodic maintenance	6.2.1 AIs should establish formal change management procedures to ensure that business continuity plans are updated for any relevant changes with proper approval and documentation. If the plan is activated, a review should be conducted after normal operations resume to identify areas for improvement. Where vendors provide critical recovery services, AIs should have formal procedures to periodically (e.g., annually) review the appropriateness of related service level agreements. 6.2.2 Each business and support function, with assistance from the business continuity function, should review its business impact analysis and recovery strategies annually to confirm that the BCP requirements remain valid under changing business and operating conditions or require updates. 6.2.3 Contact details for key staff, counterparties, customers, and service providers should be	Customers should establish procedures for updating business continuity plans, review and update business impact analyses and recovery strategies annually or as needed, and revise service level agreements (SLAs) with relevant vendors to ensure these strategies and agreements meet business continuity requirements. Customers should also promptly update contact information for key employees, counterparties, customers, and service providers. To assist customers in meeting regulatory requirements, Tencent Cloud conducts annual reviews and updates of its business continuity management system. Based on the results of business impact analyses, Tencent Cloud reviews and updates business continuity and disaster recovery plans for relevant products and services as needed. In accordance with internal business continuity management policies, Tencent Cloud also maintains an emergency contact list and assigns dedicated personnel to ensure the accuracy and validity of contact information for all parties included in the emergency plan.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		updated promptly upon receipt of change notifications.	
6. 2	Periodic maintenance	6.2.5 Copies of the BCP document should be stored at locations separate from the primary sites. A summary of key steps to take in an emergency should be made available to senior management and other key personnel and kept by them in multiple locations (e.g. office, home, briefcase or AI's website).	Customers should store business continuity plan documents in offsite backups and provide senior management and other key personnel with summary materials outlining critical steps for emergency situations, keeping copies in multiple locations. To support customers' backup requirements, including offsite backups, Tencent Cloud offers multiple storage and database services with built-in backup capabilities. For more details on backup features, please refer to **Section 4.6: Important Records Management**. Tencent Cloud has established internal procedures for maintaining and updating business continuity plans. Dedicated personnel are assigned to manage these plans and related materials, including version control and distribution of electronic and physical documents, ensuring the plans remain effective and accessible.

07 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of SA-2



For outsourcing management of AIs, the HKMA has issued two key guidelines/circulars: SA-2 Outsourcing and Guidance on Cloud Computing:

- SA-2 Outsourcing sets out the HKMA's supervisory approach to outsourcing activities and highlights important issues that AIs should address when engaging in outsourcing arrangements.
- Guidance on Cloud Computing clarifies the HKMA's supervisory expectations in relation to cloud computing and provides guidance for AIs in managing cloud-related risks.

The requirements in these two guidelines/circulars mainly focus on areas such as the capability of service providers, outsourcing agreements, confidentiality of customer data, control of outsourcing activities and related risks, contingency planning, data access rights, and other legal rights. Accordingly, in this section, Tencent Cloud will summarize and integrate the control requirements related to cloud service providers from SA-2 Outsourcing and Guidance on Cloud Computing, and explain how Tencent Cloud, as a cloud service provider, assists AIs in complying with these requirements.

No.		Domain	Summary of Controls	Tencent Cloud's Response
SA-2 Outsourcing	Guidance on Cloud Computing			
2.3.1	2	Ability of service providers	Before selecting a service provider AIs should perform appropriate due diligence. In assessing a provider, apart from the cost factor and quality of services AIs should take into account the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with AI's corporate culture and future development strategies, familiarity with the banking industry and capacity to keep pace with innovation in the market. For cloud service	Before selecting a cloud service provider and during the use of its services, customers should conduct due diligence on the provider, assess its capabilities and suitability, and consider factors specific to cloud computing. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. The following is an overview of Tencent Cloud's practices as a cloud service provider in responding to due diligence requirements across various aspects: • **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

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			providers (CSPs), AIs should also consider factors specific to cloud computing during the assessment process, including multi-tenant risk, concentration risk, supply chain risk, and the level of operational resilience. AIs may adopt a risk-based approach and, where appropriate, leverage independent third-party assessment reports and joint audit results on the cloud service provider.	recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant. • **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. • **Management Capability:** Tencent has established a risk governance framework and related procedures, continuously improving risk management measures and internal control systems. Tencent Cloud strengthens its risk culture to enhance internal risk management capabilities and ensure sustainable business development. • **Technical Capability:** Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. • **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 Mainland China, Asia-Pacific, North America, and Europe.

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
				Tencent Cloud has partnered with over 11,000 companies and delivered more than 400 industry solutions across 30+ sectors. • **Operational Resilience:** Tencent Cloud is certified under the ISO/IEC 22301 international standard for business continuity management. To ensure service availability, Tencent Cloud has developed detailed disaster recovery plans for its products and services and conducts regular drills to validate timeliness and feasibility. • **Supply Chain Security:** Tencent Cloud has implemented a comprehensive supply chain management system, including strict supplier security assessments, regular monitoring and evaluation, and clear outsourcing agreements to ensure supply chain security. • **Multi-Tenant Management:** Tencent Cloud has established a robust data management framework, adhering to the principle of "data confidentiality." Through multi-layered technical isolation measures, Tencent Cloud ensures that customer data remains segregated and inaccessible to other tenants, preventing unauthorized access, retrieval, or modification. • **Compatibility with Organizational Culture and Future Strategy:** Tencent Cloud offers customized solutions tailored to customer needs, enabling flexibility to align with different corporate cultures and strategic directions. • **Familiarity with Banking Industry:** Tencent Cloud has tailored various solutions for multiple financial

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
				institutions, providing them with a comprehensive "technology platform + security experts" service solution. These solutions effectively address security challenges, enhance security protection capabilities, and ensure compliance with security and regulatory requirements. • **Ability to Keep Pace with Market Innovation:** Tencent Cloud actively tracks market trends and technological developments, continuously launching innovative products and services to maintain its market leadership and meet evolving customer needs.
2.4.1	3、8	Outsourcing agreement	The service agreement between an AIs and its service provider should clearly specify the types of services provided, the service levels, and the responsibilities and obligations of the service provider under the contract. For cloud service providers, the agreement should also include clear provisions addressing issues specific to cloud computing. AIs should understand their own roles and responsibilities under the agreement and establish corresponding control measures. The agreement should be reviewed regularly, and consideration should be given to whether	Customers should enter into an outsourcing agreement with the cloud service provider, clearly specifying the types of outsourced services, service levels, and the responsibilities and obligations of the service provider. The agreement should be subject to regular review. 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 Tencent Cloud's offerings, the protection of user data and intellectual property, the security responsibilities and obligations of both the customer and Tencent Cloud, notifications of incidents and changes, confidentiality obligations, and information disclosure matters. Customers may also negotiate to include additional requirements in a separate contract.

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			renegotiation or updates are necessary.	
2.5.2 2.5.4	5	Customer data confidentiality	AIs should establish control measures to ensure that service providers comply with confidentiality requirements for client information and implement safeguards to protect the confidentiality and integrity of such information. These measures should include obtaining the service provider's assurance to comply with confidentiality obligations and the Personal Data (Privacy) Ordinance, segregation of client information, and granting access strictly on a need-to-know basis. For cloud service providers, AIs should implement robust controls to protect the confidentiality and integrity of client information. These include adequate identity and access management, clear and effective encryption key	Customers should implement multiple security controls to ensure the confidentiality and integrity of customer data in outsourcing arrangements. **From the perspective of compliance with confidentiality requirements,** 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. **From the perspective of access protection for customer data**, Tencent Cloud offers **Cloud Access Management (CAM)** to help customers securely and precisely manage access to Tencent Cloud products and resources. For more details, please refer to Section 5.2 "3.2 Authentication and Access Control". Customer data is classified at the highest security level within Tencent Cloud. Customers retain sole 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. **From the perspective of multi-tenant risk and data isolation**, Tencent Cloud

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			management policies, procedures and standards, sufficient controls over security configurations and cyber hygiene, effective processes for incident response and recovery, and measures to address security risks arising from multi-tenant cloud architecture. In the event of termination of the outsourcing arrangement, AIs should ensure that all client information is retrieved from the service provider or securely destroyed.	adheres to the principle of "data confidentiality" and employs multi-layered technical isolation measures, such as virtualization control layer resource access policies, internal private network isolation strategies, web console permission allocation and authentication, session IDs and access keys, to ensure that customer data remains invisible to other tenants and cannot be accessed, obtained, or altered. **From the perspective of data encryption and key management,** Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Integrated **Key Management Service (KMS)** ensures full lifecycle management of encryption keys, safeguarding data confidentiality. For more details, please refer to Section 5.2 "3.1 Information Classification and Protection". **From the perspective of security configuration and environment protection,** Tencent Cloud provides services such as **Cloud Workload Protection Platform (CWPP)**, **Cloud Security Center (CSC)**, and **Configuration Audit (Config)** to help customers detect and manage security configurations of cloud products, ensuring a secure cloud environment. Internally, Tencent Cloud has established standardized security configuration and baseline standards for network devices, firewalls, servers, databases, and applications. Tencent Cloud uses scanning tools to check configurations of operating systems, database management systems, network devices, and virtual images,

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
				continuously detecting and correcting deviations from baseline standards. **From the perspective of security incident response and recovery**, customers can use Cloud Security Center (CSC) to achieve a closed-loop security operation, including proactive threat detection, incident response, and post-event analysis through its asset center, risk center, alert center, and advanced security management. Tencent Cloud also has clear internal mechanisms and processes for information security incident response, handling, recovery, and notification. **From the perspective of termination and exit of cloud services**, if customers need to terminate agreements due to business changes or future IT planning, they can back up and migrate cloud data and production environments at any time. Tencent Cloud supports data backup and migration in standard formats, allowing customers to use the same transmission methods and protocols as during onboarding, or network services such as **Direct Connect (DC)**and **VPN Connection**, ensuring secure and reliable data transfer during offboarding. After termination, Tencent Cloud will permanently delete customer data, including copies and backups, following strict data erasure procedures, once the retention period expires. Deleted data cannot be recovered.
2.6.2 2.6.4	4	Control over outsourced activities	AIs should monitor their service providers, focusing on contractual performance, significant issues encountered, and contingency plans, and	Customers should establish monitoring procedures for outsourcing arrangements and continuously monitor outsourcing risks. To support customers' outsourcing

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			should regularly review their financial condition and risk profile. For cloud service providers, AIs should establish a comprehensive risk management framework to continuously identify, monitor, and mitigate risks specific to cloud computing. These include operational risk, cyber risk, system resilience risk, concentration risk, vendor lock-in risk, supply chain risk, data portability, availability of interoperability solutions, feasibility of adopting a multi-cloud strategy, and exit arrangements. In addition, AIs should establish escalation procedures to ensure that issues related to outsourcing are promptly reported to the management of both the AI and the service provider for timely resolution.	oversight requirements, Tencent Cloud will cooperate with third-party security audits and supervision based on actual circumstances and contractual agreements, providing dedicated personnel to assist and actively respond to audit activities initiated by customers. 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 and compliance with applicable laws, regulations, and security standards. Tencent Cloud also undergoes annual independent third-party audits and provides assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud's service organization.
2.7.1 2.7.2	6	Contingency planning	AIs and their service providers should maintain and regularly rehearse and test contingency plans, including arrangements	Customers should maintain and regularly test contingency plans and have a comprehensive understanding of the resilience capabilities of the cloud service provider, ensuring that the provider also maintains and periodically rehearses and

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			for responding to operational and system disruptions, to ensure business continuity. Where an AI's critical operations rely on cloud-based platforms, the AI should have a comprehensive understanding of the resilience capabilities of its cloud service provider and ensure that any interruption to cloud services does not compromise the AI's own operational resilience.	tests its contingency plans. To support customers in meeting regulatory requirements and ensuring continuous availability of their business operations, Tencent Cloud offers a wide range of highly available cloud products and services, including computing, networking, storage, database, container and middleware, and security services, all have the feature of high availability, as well as corresponding disaster recovery plans. Tencent Cloud has established a comprehensive business continuity management system and has obtained ISO/IEC 22301 certification for business continuity management, an internationally recognized standard. For more information on Tencent Cloud's resilience capabilities, please refer to Section 6 : How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
2.8.2	7	Access to outsourced data and other legal rights	AIs should maintain up-to-date and readily accessible records for inspection by the HKMA. AIs should ensure that agreements with service providers include provisions allowing oversight, inspection, or review of the service provider's operations and controls related to the outsourced activities. AIs should also implement measures to ensure that, during internal or external	Customers should take measures to safeguard audit rights and the Hong Kong Monetary Authority's supervisory access and regularly exercise their own audit rights to obtain assurance on the cloud service provider's risk management and security practices. **In terms of customer data access and protection,** Tencent Cloud currently operates three data centers in Hong Kong, offering a variety of cloud computing services including cloud servers, cloud databases, and CDN. Hong Kong customers can choose to store and process their data locally within Hong Kong. Tencent Cloud's storage services support data encryption, backup, migration, and access control management, meeting both

No. SA-2 Outsourcing	No. Guidance on Cloud Computing	Domain	Summary of Controls	Tencent Cloud's Response
			audits or HKMA reviews, information stored in the cloud and related risk management controls can be accessed promptly and accurately within Hong Kong. AIs should regularly exercise their audit rights to obtain reasonable assurance regarding the cloud service provider's risk management and security standards.	customer and regulatory requirements. **In terms of customer audits and regulatory reviews,** Tencent Cloud will cooperate with third-party security audits and supervision based on actual circumstances and contractual agreements, providing dedicated personnel to assist and actively respond to audit activities initiated by customers.

08 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-E-1

TM-E-1 Risk Management of E-banking provides guidance to AIs on potential risks associated with electronic banking and the corresponding risk management measures. The requirements relevant to cloud service providers mainly cover areas such as independent assessment and penetration testing, confidentiality and integrity of information, internet infrastructure, application system security, threat monitoring and vulnerability assessment, incident response and regular drills, capacity planning, performance monitoring, system availability and resilience, and handling of system disruptions.

In this section, Tencent Cloud will summarize and consolidate the control requirements related to cloud service providers under TM-E-1 Risk Management of E-banking and explain how Tencent Cloud, as a cloud service provider, assists AIs in meeting these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.3	Independent assessment and penetration tests	3.3.1 AIs' senior management should establish clear policies and accountability to ensure a rigorous independent assessment is conducted before launching any new e-banking delivery channel or making major enhancements to existing services. The assessment should verify compliance with applicable regulatory guidance and confirm that adequate risk management controls are in place. Independent assessments must be performed by trusted assessors with the necessary expertise and independence. Reports should be submitted to the HKMA upon request. 3.3.2 Senior management should ensure that qualified independent parties perform regular penetration tests, at least annually, covering Internet banking and any financial services delivered over the Internet or wireless networks. Tests should be carefully planned to avoid undue disruption to production systems. 3.3.3 AIs should conduct	Customers should establish clear policies and procedures to ensure that independent assessments are conducted by qualified and independent assessors before launching any new e-banking services or making significant enhancements to existing services. In addition, penetration testing and risk assessments should be performed at least annually. **In terms of independent assessment and risk evaluation,** Tencent Cloud actively responds to customer-initiated reviews or assessment activities and provides dedicated support throughout the process. In addition, Tencent Cloud undergoes regular independent third-party professional audits and issues assurance-based System and Organization Controls (SOC) reports to cloud users, independent auditors, regulators, company shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. Furthermore, the Tencent Cloud 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. **In terms of penetration testing**, Tencent Cloud offers **Penetration Testing Services (PTS)** to customers, simulating attack techniques and vulnerability discovery methods that hackers might use. These tests are performed using controlled, non-destructive approaches to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		formal risk assessments at least annually to ensure adequate risk management controls for Internet banking and financial services delivered online. Assessments should consider changes in risk profile, emerging vulnerabilities, and other relevant risks, and results should be endorsed by senior management with timely remediation of material issues.	thoroughly assess the security of target systems, identify weaknesses in systems and network devices, and provide hardening recommendations to help customers enhance system security. Additionally, the Tencent Cloud security team regularly conducts large-scale, end-to-end penetration tests and performs targeted tests before new product launches or major changes. Test results are communicated via security tickets to the responsible departments, which promptly remediate vulnerabilities or implement compensating controls to ensure that exploitable issues identified during testing are properly addressed.
4.4	Customer security	4.4.5 AIs are reminded of the need to comply with the Personal Data (Privacy) Ordinance and any relevant codes of practice / guidelines or guidance issued or published by the Privacy Commissioner for Personal Data or the Office of the Privacy Commissioner for Personal Data (PCPD) from time to time.	Customers should comply with the Personal Data (Privacy) Ordinance and relevant guidelines. To support customers in meeting regulatory requirements, Tencent strictly adheres to laws and regulations related to personal information protection and data security in the jurisdictions where it operates. The Tencent Cloud Legal team continuously identifies and collects compliance requirements relevant to Tencent Cloud services, maintains a corresponding legal and regulatory inventory, and updates it regularly. Tencent has established a user-centric privacy protection framework. By improving privacy compliance assessment processes and tools, and integrating international standards, technological innovation, and employee training, Tencent embeds privacy protection into multiple aspects of corporate culture to ensure the highest level of privacy protection for customers.
5.1	Confidentiality and integrity of information	5.1.1 AIs should adopt secure and internationally recognized strong encryption algorithms to protect the confidentiality of customer information transmitted over external networks, including the Internet, as well as highly	Customers should use secure, strong encryption algorithms to protect sensitive information during storage and transmission, adopt robust key management measures to safeguard encryption keys, and implement mechanisms to maintain and verify data integrity. **For data storage protection,** Tencent Cloud's storage and database products support data

No.	Domain	Summary of Controls	Tencent Cloud's Response
		sensitive information stored or transmitted over internal networks. Sound key management measures should be implemented to protect encryption keys. The implementation of encryption controls for e-banking should be carefully evaluated from time to time and improved or updated whenever necessary. 5.1.2 AIs should implement sufficient controls to maintain and verify the integrity of data processed by online banking systems.	encryption using secure, high-strength algorithms. Encryption keys are managed through the **integrated** Key Management Service (KMS), which provides full lifecycle management. Key Management Service (KMS) uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect keys and supports key rotation to reduce the risk of compromise or misuse. Invalid, expired, or compromised keys are securely deleted using reliable methods, and once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. 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 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. Tencent Cloud has established security management specifications for encryption algorithm usage and key management, defining security requirements for key application, generation, storage, usage, transmission, update,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and destruction. All key lifecycle operations follow dual-control principles, strict handover, proper custody, and timely updates. During key usage, Tencent Cloud enforces segregation of duties, rigorous approval processes, real-name operations, and maintains detailed key operation logs with regular audits. For encryption during data storage and transmission, Tencent Cloud requires internal teams to comply with international cryptographic standards and regulations, using high-security algorithms such as AES-256 and ensuring key lengths meet security requirements. Tencent Cloud has conducted internal security compliance self-assessments in accordance with Hong Kong Monetary Authority's Guideline on Sound Practices for Customer Data Protection and engaged independent third-party evaluations. Assessment results confirm that Tencent Cloud's internal controls meet relevant regulatory requirements.
5.2	Internet infrastructure	5.2.1 AIs should establish a secure Internet infrastructure (including the design of the demilitarized zone and configuration of the relevant devices, as well as intrusion detection controls) to support their Internet banking system. Moreover, AIs should implement adequate security measures for the internal networks and network connections to external parties, and proper patch management procedures for systems and infrastructure components.	Customers should establish a secure internet infrastructure, implement security measures for internal and external network connections, and adopt patch management procedures for systems and infrastructure components. To support customers in meeting regulatory requirements, Tencent Cloud provides a mature network security architecture featuring multiple protection mechanisms, including firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS mitigation, network segmentation, and web application security. These mechanisms enable timely detection, filtering, and blocking of malicious traffic to safeguard Tencent Cloud's network. Tencent Cloud also offers services such as **Virtual Private Cloud (VPC)**, **Cloud Firewall (CFW)**, **and Web Application Firewall (WAF)** to help customers implement demilitarized zone (DMZ) designs, intrusion detection, and other network perimeter security measures. For more details on Tencent Cloud's

No.	Domain	Summary of Controls	Tencent Cloud's Response
			network security and related products, please refer to Section 5.5 "Communication Network". Tencent Cloud has established standardized network security configuration and baseline standards for network devices, firewalls, host operating systems, databases, and application systems. Using configuration scanning tools, Tencent Cloud continuously detects deviations from these standards in operating systems, database management systems, and virtual images. Identified deviations automatically generate security tickets, which are sent to responsible teams for timely remediation. Tencent Cloud also regularly reviews security policies and parameter settings for routers, firewalls, and network servers to ensure effectiveness. Additionally, Tencent Cloud operates an internal network monitoring system for routers, firewalls, and network servers, and deploys Endpoint Detection and Response (EDR) tools to comprehensively 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. For more details on system and infrastructure security, please refer to Section 5.2 "3.4 System Security".
5.3	Application system security	5.3.1 AIs should put in place an adequate level of application system security in respect of their Internet banking system, including any Apps, covering at least application design and development, testing and implementation. 5.3.2 Before launching any Internet banking system or system changes, an adequate application system source code review. Such review should be conducted by an appropriate party with relevant expertise and the party should also be	Customers should ensure an adequate level of application security throughout the lifecycle of their online banking systems and conduct source code reviews before launching any online banking system or implementing system changes. To assist customers in managing the application system lifecycle, Tencent Cloud provides **Cloud Native Build (CNB)** developer tools. CNB is based on the Docker ecosystem and abstracts environments, caches, and plugins using declarative syntax to help developers build software more efficiently. CNB offers a complete developer tool chain, including code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and customizable task sets.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		independent of the staff who developed the application system.	These capabilities enable full lifecycle support from requirements to deployment and facilitate agile development management. Tencent Cloud has established secure development standards and applies these standards across all stages of the product lifecycle—including requirements, design, development, testing, delivery, and operations—embedding information security and privacy protection principles throughout. This ensures that cloud products maintain robust security controls during their entire lifecycle. In addition, Tencent Cloud has implemented management standards for product and configuration changes. Under these standards, all types of program changes are subject to testing, business impact analysis, rollback planning, and approval by responsible personnel before deployment. For operational changes that may affect customers, Tencent Cloud promptly issues change notifications through official channels such as the website and in-platform messages. For more details on application lifecycle security and change management, please refer to Section 5.3 "System Development and Change Management".
5.4	Threat monitoring and vulnerability assessment	5.4.1 AIs should establish a systematic monitoring process to closely monitor emergent security threats that are relevant to their Internet infrastructure, application systems and other relevant system components and operations. 5.4.2 AIs should also utilize automated tools (supplemented by manual techniques if needed) to perform periodic vulnerability assessment to detect security vulnerabilities in their Internet infrastructure	Customers should closely monitor security threats related to their internet infrastructure, application systems, and system components, use automated tools to conduct regular vulnerability assessments, and adopt effective measures to address risks arising from identified threats or vulnerabilities. **In terms of threat monitoring,** Tencent Cloud provides customers with a one-stop security management platform —**Cloud Security Center (CSC)** —which supports periodic detection of six major risks: port risks, vulnerability risks, weak password risks, content risks, cloud resource configuration risks, and service exposure risks. CSC continuously monitors enterprise security status and integrates logs from Cloud Firewall,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and relevant Internet banking systems. 5.4.3 AIs should adopt a risk-based approach to addressing the risks arising from the security threats or vulnerabilities identified.	Web Application Firewall, and Host Security for auditing, analysis, aggregation, unified display, and tracking of alerts. Tencent Cloud has also established detailed operational security "red lines" and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base combined with three AI engines—credit, behavior, and content—to deliver an automated operational security auditing tool. This tool promptly identifies abnormal behaviors and triggers real-time alerts. Additionally, Tencent Cloud operates an internal network monitoring system for routers, firewalls, and network servers, and deploys Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. Identified security issues are tracked and resolved through a ticketing system. **To meet regulatory requirements for periodic vulnerability identification and assessment**, customers can use **Vulnerability Scanning Service (VSS)** to detect and assess risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and offers professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection for customer assets, providing professional remediation advice to reduce security risks. VSS also integrates with other Tencent Cloud products such as Host Security and Web Application Firewall to create a closed-loop process from risk detection to mitigation. Tencent Cloud has established internal threat and vulnerability management procedures to ensure timely identification of threats and vulnerabilities affecting infrastructure and information systems, followed by appropriate remediation measures. Tencent Cloud conducts regular vulnerability scans and communicates results to responsible

No.	Domain	Summary of Controls	Tencent Cloud's Response
			departments for prompt risk mitigation and impact assessment. After internal review, Tencent Cloud issues vulnerability notifications to customers via official channels such as website announcements and in-platform messages. Notifications include, but are not limited to, vulnerability descriptions, scope and severity, control measures implemented by Tencent Cloud, remediation recommendations, and detailed operational guidance.
8.2	Incident response and periodic drills	8.2.1 AIs should put in place formal incident response and management procedures for timely reporting and handling of different kinds of incidents (including suspected or actual security breaches, cyber-attacks, frauds or service interruptions). 8.2.2 A communication strategy should be formulated by the senior management to ensure that consistent and up-to-date messages are conveyed to all relevant parties (e.g. customers, media and business partners) on a timely basis and notify the customers affected, or likely to be affected, and inform them of the key facts relating to the incident and the steps that customers may take. 8.2.4 AIs should also formulate and regularly undertake assessment and practice drills on their incident response and management procedures to ensure sufficient management oversight, adequate capacity and effective incident management capability.	Customers should establish incident response and management procedures, define clear communication strategies, and conduct regular incident response drills to ensure timely reporting and handling of incidents that may affect their electronic banking services. To support customers in meeting regulatory requirements, Tencent Cloud has developed an Information Security Incident Management Standard and established mechanisms and processes for reporting, responding to, and handling security incidents. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyses and classifies them based on factors such as the nature of the incident, data sensitivity, and impact scope, and promptly notifies the responsible personnel for follow-up actions. For security incidents that may affect customers, Tencent Cloud, after internal review, communicates the handling and analysis results through appropriate channels and provides technical support to assist customers in implementing remedial measures to minimize potential losses. To ensure the effectiveness and timeliness of incident response processes, Tencent Cloud business units regularly conduct emergency drills for security incidents and provide technical training to security team members based on evolving technologies and threat landscapes. This

No.	Domain	Summary of Controls	Tencent Cloud's Response
			ensures that employees understand and comply with the latest security requirements, operational procedures, and best practices. Tencent Cloud offers online and telephone support channels on its official website, enabling customers to report issues encountered while using Tencent Cloud services and providing 24/7 technical assistance.
9.1 9.4	Service level of e-banking for customers and System resilience	9.1.2 AIs should ensure that their controls relating to system resilience and their capacity planning for e-banking cover all related systems and infrastructure components within their institutions as well as those of any relevant service providers to ensure stability, performance and continued system availability of e-banking to the relevant customers. 9.4.1 AIs should ensure that there is no single point of failure in the systems/infrastructure components nor unnecessary connections or dependency upon less critical systems. It is important that the actual effectiveness of the resilience of the system should be properly verified and tested. 9.4.2 If the system resilience of AIs depends on the cooperation of external service providers, they should maintain an adequate level of monitoring of the system resilience of these service providers and understand their contingency planning arrangements. If the	AIs should ensure the continuous availability of their electronic banking systems, implement control measures for related systems and infrastructure components, and regularly validate and test system resilience. If system resilience depends on external service providers, AIs should maintain adequate monitoring of the providers' resilience capabilities. To support customers in meeting regulatory requirements and ensure the continuous stability and availability of their business 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 requirements and service level commitments. Its cloud products and services—including compute, network, storage, database, container and middleware, and security services—are designed with high availability features and corresponding disaster recovery plans. Tencent Cloud also actively responds to customer-initiated audits or reviews and provides dedicated assistance as needed. Tencent Cloud has obtained ISO/IEC 22301 certification for its Business Continuity Management System and has established a comprehensive internal framework for business continuity. This includes regular disaster recovery drills and testing to ensure robust disaster recovery capabilities, rapid response, and efficient restoration of systems and services.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		service providers concerned are AIs' outsourcing agents, AIs should assess the system resilience controls of the service providers as part of the assessment of their own system resilience.	For more details on Tencent Cloud's service and infrastructure resilience, please refer to Section 6: How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
9.2	Capacity planning	9.2.1 A thorough review of the system capacity of the relevant systems and infrastructure should be conducted from time to time to identify any potential weaknesses that may affect the stability and performance of e-banking. Regular capacity planning and performance reports should be produced for senior management's attention. Any necessary enhancement measures to rectify the identified weaknesses should also be implemented promptly to avoid possible system instability. 9.2.2 Capacity planning guidelines should be established, clearly specifying system utilization thresholds and corresponding preventive measures. A capacity planning methodology should also be developed to help estimate future capacity requirements and translate business needs into IT capacity plans. 9.2.3 A fast-track software and hardware procurement process should be formulated, including prior arrangements with relevant software and hardware providers to enable system capacity upgrades within a	AIs should establish capacity planning guidelines that define system utilization thresholds, corresponding preventive measures, capacity planning and estimation methods, and fast-track procedures for software and hardware procurement. AIs should also regularly review system capacity for relevant systems and infrastructure, conduct end-to-end stress testing, identify weaknesses in systems and infrastructure components, and implement timely improvements and corrective actions. **To support customers in efficient capacity planning and adjustment,** Tencent Cloud provides **Auto Scaling (AS)** services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs, policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. **When reviewing system capacity or conducting stress testing, c**ustomers can also use Cloud Pressure Testing (PTS) services to simulate large-scale real-world traffic scenarios, comprehensively validating system availability and stability. PTS supports millions of concurrent requests across multiple regions, traffic recording, scenario orchestration, traffic customization, and advanced scripting, enabling accurate stress testing based on business models and early identification of performance issues. Tencent Cloud has established internal capacity management procedures to forecast capacity

No.	Domain	Summary of Controls	Tencent Cloud's Response
		short period when needed. Adequate end-to-end system stress testing should be conducted with full coverage of all relevant systems and infrastructure components to identify potential performance bottlenecks in advance.	requirements based on business operational needs and to develop annual capacity management plans. In addition, Tencent Cloud uses an internal capacity monitoring platform to track real-time capacity utilization and identify usage trends.
9.3	Performance monitoring	9.3.1 Regardless of the scale of e-banking, an automated performance monitoring and alert system, which covers all critical systems and infrastructure components supporting e-banking, should be in place so that any potential system interruption or performance degradation both during or after office hours could be detected and handled by designated staff in a timely manner.	AIs should implement automated performance monitoring and alerting systems for all critical systems and infrastructure components that support electronic banking. **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. **For infrastructure monitoring and management aspects** , Tencent Cloud has deployed internal network monitoring systems to monitor and alert on network devices such as routers, firewalls, and servers. It also uses Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. The EDR solution supports antivirus and intrusion detection, security baseline checks, vulnerability scanning, and compliance audits for command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviors, and issues are tracked and resolved through the ticketing system.

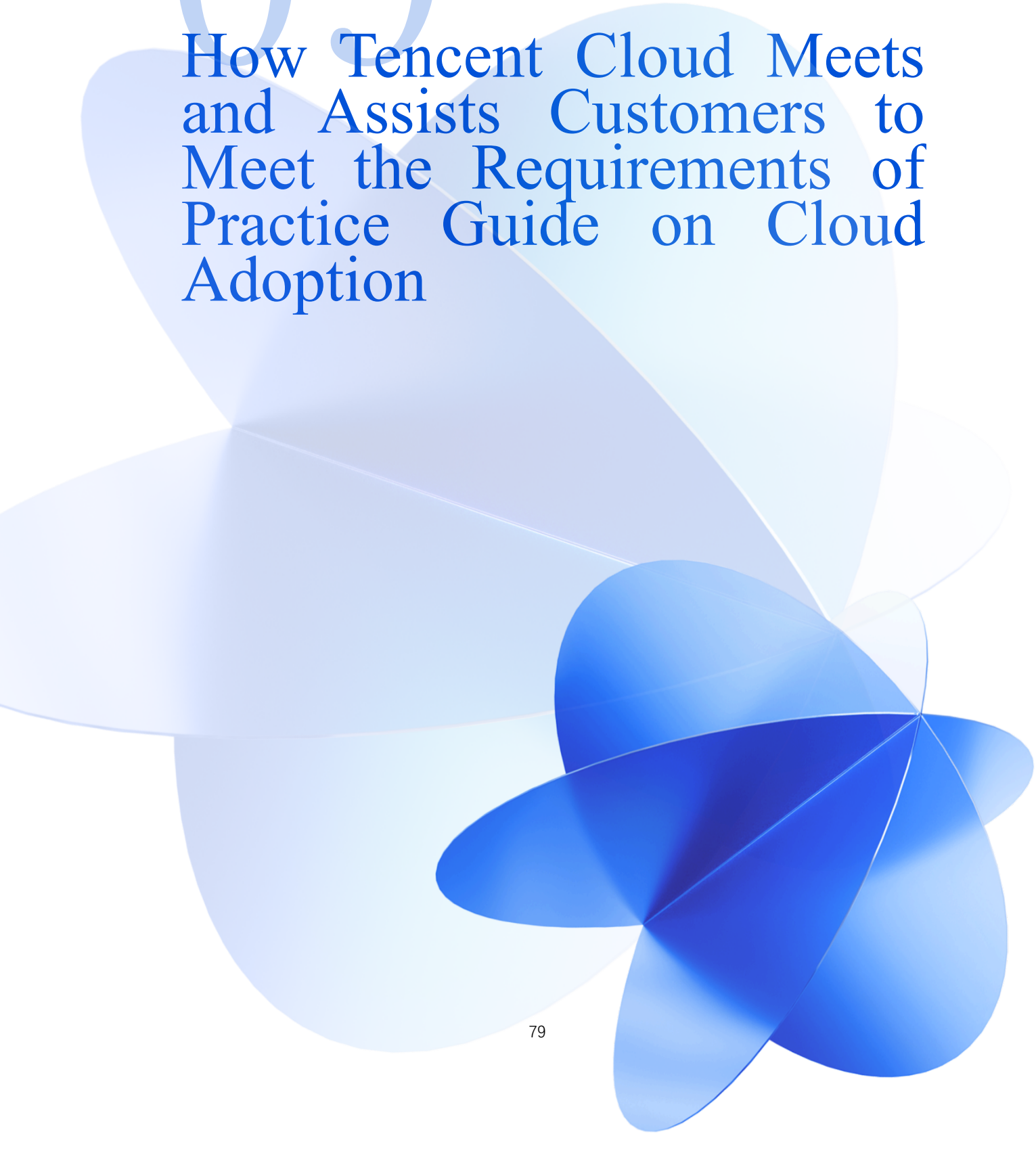
No.	Domain	Summary of Controls	Tencent Cloud's Response
9.5	Controls for coping with system disruptions	9.5.1 AIs' IT function should establish a service level agreement with business lines covering availability of e-banking systems. Against this system availability benchmark, AIs should maintain and service the relevant IT facilities and equipment in accordance with industry practices and suppliers' recommended service intervals and specifications. Moreover, AIs should formulate and undertake regular practice drills to test the relevant IT disaster recovery plan and procedures to ensure that their e-banking services can be resumed within a short period of time and in accordance with the AIs' business recovery requirements, taking into account the duration required for trouble-shooting, problem fixing and switching over to the back-up e-banking systems if needed. 9.5.2 AIs should take appropriate measures having regard to common issues that could lead to disruptions of e-banking. Moreover, AIs should implement proper precautionary measures before and during scheduled maintenance or drills.	AIs should establish service level agreements (SLAs) covering the availability of electronic banking systems, regularly maintain and service relevant IT facilities and equipment, and develop IT disaster recovery plans and procedures, which should be tested through regular drills. **For service level and availability management aspects,** Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud services , the expected service levels, and the respective security responsibilities and obligations of both Tencent Cloud and its customers. **For infrastructure maintenance,** Tencent Cloud assigns on-site data center personnel to regularly inspect critical equipment in server rooms, following predefined procedures to record inspection results, report anomalies, and resolve identified issues promptly to eliminate security risks and ensure stable equipment operation. **In terms of IT disaster recovery planning and drills ,** Tencent Cloud is certified under the ISO/IEC 22301 international standard for business continuity management. To ensure service availability, Tencent Cloud has developed detailed disaster recovery plans for its products and services and conducts regular drills to validate timeliness and feasibility. Tencent Cloud provides customers with **Tencent Security Smart Advisor (TSA)** services, which offer fault injection scenarios across IaaS to PaaS layers, along with industry-specific drill templates. These resources help customers efficiently reuse proven solutions tailored to their business needs, enhancing system availability and resilience. For more details on disaster recovery planning and drills, please refer to Section 6: How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Planning.
9.5	Controls for coping with system disruptions	9.5.3 Moreover, AIs should implement adequate controls to promptly detect and respond to the threats posed by distributed denial-of-service (DDoS) or other cyber attacks that could directly or indirectly cause disruptions to e-banking systems. These controls should be validated (e.g. testing at point of service activation or a production-like system environment) and periodically reviewed to ensure their ongoing effectiveness against any emerging techniques in DDoS attacks.	AIs should implement measures to promptly detect and respond to DDoS attacks and other network threats that may directly or indirectly disrupt electronic banking systems. These control measures should be validated and reviewed regularly. Customers can use Tencent Cloud's **Anti-DDoS** service. This service leverages abundant and high-quality DDoS mitigation resources, combined with continuously evolving proprietary and AI-driven traffic cleansing algorithms, to ensure stable and secure business operations. Anti-DDoS offers multiple protection solutions, including basic DDoS protection for cloud servers and load balancers—supporting real-time traffic monitoring, attack mitigation, and daily security operations—as well as high-availability, high-reliability services such as DDoS High Defense IP, designed to prevent service disruptions and financial losses caused by large-scale attacks. Customers may also choose **EdgeOne DDoS Protection**, an edge security acceleration platform that uses Anycast routing technology to provide Layer 3/Layer 4 traffic-based DDoS protection. EdgeOne monitors network traffic in real time and initiates traffic cleansing upon detecting an attack. Its protection capabilities include preset defense strategies and advanced filtering algorithms based on attack profiling, behavioral analysis, and AI recognition, enabling detection and mitigation of various DDoS attack types. For businesses with high DDoS risk exposure, long connection requirements, or custom traffic control needs, EdgeOne offers dedicated DDoS protection through exclusive cleansing centers to enhance defense capabilities. **To support customers in meeting regulatory requirements and defending against DDoS attacks**, Tencent Cloud has deployed firewalls, intrusion detection/prevention systems (IDS/IPS),

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and DDoS protection tools, and conducts regular DDoS defense drills. Tencent Cloud has also performed internal compliance self-assessments in accordance with Hong Kong Monetary Authority's Guidance on anti-DDoS protection and engaged independent third-party evaluations. Assessment results confirm that Tencent Cloud's internal control measures meet relevant regulatory requirements.

09

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Practice Guide on Cloud Adoption



The Hong Kong Monetary Authority (HKMA) issued the Practice Guide on Cloud Adoption in January 2026, providing more detailed supervisory directions and guidance for Authorized Institutions on their adoption of cloud technology. By sharing industry best practices, the Practice Guide aims to assist AIs in managing cloud-related risks through governance approaches and principles commensurate with their risk profiles and the materiality of cloud arrangements, thereby strengthening their robust risk management frameworks. This Practice Guide attests to the HKMA's continued support for AIs to adopt cloud in a responsible manner, under our "Fintech 2030" strategy. The requirements cover multiple areas, including governance and oversight, risk assessment and due diligence, cloud service provider contractual provisions and related controls, cloud resilience and exit strategy, cloud security and data protection, incident management, ongoing monitoring, and workforce strategy and empowerment.

In this section, Tencent Cloud summarizes the control requirements in the Practice Guide on Cloud Adoption that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists Authorized Institutions in meeting these requirements.

9.1 Governance and Oversight

No.	Domain	Summary of Controls	Tencent Cloud's Response
IC	Cloud record management	Effective oversight and risk management of cloud initiatives rely on maintaining complete, accurate, and up-to-date records of an AI's cloud resources and arrangements. AIs should ensure that such records provide a sound basis for monitoring risks, managing incidents, supporting planning and decision making, and demonstrating compliance with applicable regulatory requirements.	Customers should maintain complete and accurate records of the cloud resources and their configurations to ensure effective supervision and risk management of the cloud project. In terms of cloud resource management, the Tencent Cloud console provides resource management functionality, enabling customers to browse and search for cloud resources under their account on the resource management page. With the appropriate view permissions, they can query all resources under the respective view. In addition, **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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management. CSC includes the Asset Security Center function, which enables customers to achieve automated dynamic inventory of cloud assets (including CVM, COS, Tencent DB, CLB instances) and conducts unified management of asset security risks through multiple security dimensions such as cloud configuration risks, vulnerabilities, and security events, thereby reducing the risk of "shadow IT" on the cloud. To support customers in 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. **In terms of configuration management**, 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.

9.2 Risk Assessment and Due Diligence

No.	Domain	Summary of Controls	Tencent Cloud's Response
2A	Pre-adoption risk assessment	AIs should conduct a pre-adoption risk assessment that is commensurate with the nature, scale, complexity and criticality of the intended cloud adoption. As part of this process, particular attention should be paid to the following factors: data location, jurisdictional and regulatory requirements, reliance on external or internal service providers and their supply chain dependencies, and multi-tenancy arrangements. AIs should also explicitly consider concentration risk arising from reliance on a limited number of CSPs. In Software as a Service (SaaS) models, the reduced direct control over data and operations should also be considered.	Before adopting cloud technology, customers should conduct a risk assessment of the nature, scale, complexity and significance of cloud technology. The content of the risk assessment includes but is not limited to data location, jurisdictional and regulatory requirements, reliance on external or internal service providers and their supply chain dependencies, and multi-tenancy arrangements, security and data protection, concentration risk, and control of data and operations. Tencent Cloud assigns dedicated personnel to respond to customers' risk assessment and due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. 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. Below is an overview of Tencent Cloud's capabilities in various aspects of due diligence as a cloud service provider: • **Data Locations** 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 currently operates three data centers in Hong Kong, offering a variety of cloud computing services including cloud servers, cloud databases, and CDN. Hong Kong customers can choose to store and process their data locally

No.	Domain	Summary of Controls	Tencent Cloud's Response
			within Hong Kong. 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. • **Jurisdictional and Regulatory Requirements** 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. 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, demonstrating that Tencent Cloud's security and privacy protection capabilities meet relevant certification standards and industry best practices. Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			undergoes professional third-party audits annually. • **Resilience and Service Performance** 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. 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. • **Reliance on External or Internal Service Providers and Their Supply Chain Dependencies** Tencent Cloud's core key technologies are all developed and built in-house, without reliance on external suppliers. At the hardware equipment and network infrastructure level, a multi-vendor architecture is adopted, balancing technological autonomy and supply chain redundancy security. This effectively mitigates risks associated with single-vendor dependency and enhances the overall resilience of the system. Tencent Cloud publishes the online **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 HKMA 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. • **Multi-tenancy Arrangements** 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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• **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. • **Security and Data Protection** Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data content. Tencent Cloud 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. 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.
2B	Provider selection and due diligence	AIs should proceed to shortlist potential vendors through a robust evaluation and due diligence process that helps the AI determine whether a given vendor would be able to deliver the required services in a secure	Customers should proceed to shortlist potential vendors through a robust evaluation and due diligence process. Customers can also use internationally recognized certifications, audit reports and other independent third-party assessments as proof of the due diligence. Tencent Cloud assigns dedicated personnel to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and reliable manner, and in compliance with applicable laws and regulatory requirements. To enable better outcomes, AIs should apply a consistent, well-defined methodology during the process that may draw on internationally or nationally recognised certifications, audit reports, and other independent third-party assessments as part of their due diligence to validate the CSP's control environment and compliance capabilities.	respond to customers' risk assessment and due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. 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.
2C	Ongoing reviews of risk assessment frameworks and CSP arrangements	AIs should conduct periodic reviews should be undertaken to assess whether initial assumptions remain valid, whether a CSP's security, compliance, or financial condition has materially changed, and whether engagement of the CSP continues to align with the AI's risk appetite and regulatory obligations. These periodic reviews should be conducted at intervals commensurate with the criticality of the cloud arrangements, and whenever significant incidents, regulatory findings, or material changes arise. In tandem, the AI's risk assessment framework and due diligence methodology should also be subject to periodic review and timely updates to take into account, as appropriate, changes in business models, technology,	Customers should regularly review cloud service providers to assess whether the previous conclusions are still valid and conduct reviews after major incidents. Tencent Cloud assigns dedicated personnel to respond to customers' risk assessment and due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		regulatory expectations, and the threat landscape, as well as lessons learned from incidents, scenario testing, industry practices, and supervisory feedback.	

9.3 Cloud Service Provider Contractual Provisions and Related Controls

No.	Domain	Summary of Controls	Tencent Cloud's Response
3A	CSP contractual arrangements and safeguards	AIs should establish clear and enforceable contractual arrangements with CSPs. AIs should subject contractual arrangements to regular review to verify that they remain fit-for-purpose, taking into account relevant factors, such as the CSP's performance, regulatory requirements and the latest operating landscape.	Customers should sign clear and executable contractual arrangements with the cloud service provider. Customers should also review and update the contractual arrangements regularly to ensure they meet the actual needs. Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure requirements. Customers may also negotiate additional requirements to be included in separate agreements.
3B	Subcontracting management	Contractual provisions should not just be limited to the direct relationship between the AI and the CSP but should also extend to subcontracting and all downstream service providers, where appropriate. Such provisions should ensure that the CSP remains contractually liable for the performance and compliance of its subcontractors, and that accountability, transparency, and enforceability are	Customers should ensure that the contractual provisions signed with the service provider cover all its subcontractors as well as all appropriate downstream service providers, to ensure that the service provider is responsible in the contract for the performance and compliance of its subcontractors. Customers should also establish supervision and monitoring of the cooperation between the service provider and its subcontractors. For sub-processing scenarios, Tencent Cloud publishes the online **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, these agreements

No.	Domain	Summary of Controls	Tencent Cloud's Response
		maintained across the entire supply chain. AIs should retain rights of notification, approval, and objection over material subcontracting arrangements. In addition, AIs should seek to secure contractually enforceable commitments that equivalent resilience, security, data protection, and regulatory obligations will be applied consistently across every tier of third-party and subcontracting arrangements, to ensure that operational continuity and control adequacy are maintained at all levels. AIs should also put in place effective arrangements to oversee and monitor CSPs' engagement of subcontractors.	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 HKMA 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.
3C	Shared responsibility model	As part of or leveraging contractual and subcontracting provisions, AIs should agree, maintain and ensure the continued effectiveness of a shared responsibility model with CSPs. This model should clearly distinguish between the CSP's responsibility for the "security	Customers should clearly specify the security sharing responsibility model in the contract signed with the cloud service provider, explaining the division of responsibilities between the cloud service provider and the customer in the cloud service, and conducting regular reviews and updates of this shared responsibility model. Tencent Cloud embraces the openness and shared nature of cloud computing services, continuously

No.	Domain	Summary of Controls	Tencent Cloud's Response
		of the cloud" and the AI's responsibility for the "security in the cloud". It should set out how responsibilities are divided under different cloud service models (e.g. IaaS, PaaS, SaaS), allocate control ownership in a way that avoids gaps or overlaps, and reflect evidence of the CSP's capability to meet its assigned obligations. The model should also be reviewed and updated as services, technologies, or risk profiles evolve, ensuring ongoing alignment with the AI's risk appetite, security and resilience objectives.	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.
3D	Standards and certification assurance	AIs should require CSPs to demonstrate compliance with recognised international and national standards that are proportionate to the nature and criticality of outsourced workloads. Certification or attestation should, where available, be valid, relevant, and independently issued by accredited bodies. Where such certifications or attestations are unavailable, insufficient in scope, or outdated, AIs should consider alternative assurance through reliable third-party assessments or equivalent measures to ensure CSP controls continue to meet regulatory expectations and AIs' own requirements.	Customers should require the service provider to be able to prove that it complies with recognized international and national standards. If such certifications or proofs are unavailable, customers can consider using a third-party assessment to ensure that the control measures of the cloud service provider meet regulatory requirements and customers' own requirements. Tencent Cloud strictly complies with the laws and regulations of the jurisdictions where it operates. Through independent third-party audits and assessments, it has obtained numerous security and privacy compliance certifications and qualifications, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. Specifically for Hong Kong, Tencent Cloud has successfully passed the IT compliance audit for Hong Kong Special Administrative Region financial industry conducted by an independent third party. Customers can independently download the latest report from the Tencent Cloud Compliance Document Center. These certifications

No.	Domain	Summary of Controls	Tencent Cloud's Response
			demonstrate that Tencent Cloud's security and privacy protection capabilities meet relevant certification standards and industry best practices. For more detailed information about the authoritative certifications obtained by Tencent Cloud and the completed third-party independent assessments/audits, please refer to Section 2 "Tencent Cloud Security and Privacy Compliance" of this guide.

9.4 Cloud Resilience and Exit Strategy

No.	Domain	Summary of Controls	Tencent Cloud's Response
4A	Cloud resilience	AIs should ensure that their cloud arrangements are resilient by design and can continue to support their critical operations under severe but plausible scenarios. Resilience arrangements should be commensurate with the criticality of the workloads deployed, incorporating redundancy in geography and infrastructure to minimise single points of failure and enable timely recovery or failover. To address concentration and geopolitical risks, AIs should assess and mitigate dependencies on individual CSPs or specific geographic locations. More stringent safeguards should be applied where workloads are critical, to ensure that reliance on any single CSP or location does not compromise the AI's ability to maintain critical operations.	Customers should ensure the resilience of the cloud service architecture by implementing redundancy in terms of geography and infrastructure, which can minimize single-point failures and ensure that critical business operations can be supported in extreme circumstances. Additionally, customers should assess and mitigate dependencies on individual cloud service providers or specific geographical locations to mitigate concentration risks and geopolitical risks. 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 currently operates three data centers in Hong Kong, offering a

No.	Domain	Summary of Controls	Tencent Cloud's Response
			variety of cloud computing services including cloud servers, cloud databases, and CDN. Hong Kong customers can choose to store and process their data locally within Hong Kong. Tencent Cloud offers a wide range of highly available cloud products and services, including computing, networking, storage, databases, container and middleware, and security services, all have the feature of high availability, as well as corresponding disaster recovery plans. Tencent Cloud has established a comprehensive business continuity management system and has obtained ISO/IEC 22301 certification for business continuity management, an internationally recognized standard. For more information on Tencent Cloud's resilience capabilities, please refer to Section 6 : How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
4B	Business continuity planning	AIs should ensure that a comprehensive business continuity management framework is in place. The framework should be aligned with the AI's strategic objectives, risk appetite, and regulatory obligations, and include continuity plans for cloud services, supporting backup and recovery arrangements, and measures to assess and enhance CSPs' resilience. These arrangements should mitigate the risk of downtime, data loss, and other disruptions affecting cloud platforms that underpin critical operations. The disaster recovery arrangements should be subject to regular oversight, supported	Customers should establish a business continuity management framework that is consistent with its strategic objectives, risk appetite, and regulatory obligations and include continuity plans for cloud services, supporting backup and recovery arrangements. Additionally, customers should assess the business continuity management of the cloud service provider. Customers should conduct regular tests of the disaster recovery plan and, when necessary, conduct tests together with the cloud service provider. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		by periodic testing of recovery plans and assessments of CSPs' capabilities.	based on analysis results. Regular drills are conducted to validate plan effectiveness. 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. For more details on business continuity, refer to Section 6 : How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
4C	Portability and interoperability	AIs should also plan for long-term flexibility by designing cloud workloads to be portable (i.e. the capability to migrate applications and data between environments with minimal modification) and interoperable with other platforms (i.e. the capability of different systems or CSPs to exchange and use information reliably) proportionate to their criticality. This approach enables workloads and data to be migrated securely and efficiently across environments when required, providing the flexibility to redeploy critical functions in response to strategic changes, major disruptions, or other severe but plausible scenarios that may	Customers should consider portability and interoperability when designing cloud workloads, ensuring that the workloads and data can be safely and efficiently migrated between different environments when needed, and should also take this aspect into account when selecting a cloud service provider. In addition, customers should formulate exit strategies, clearly defining goals, risk indicators, migration arrangements for contract termination, and trigger conditions for initiating the exit, to ensure that the business can continue to operate when the cloud service arrangement is terminated. The exit plan should be subject to regular review and testing. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		affect the current service environment. These aspects should be considered during CSP selection and maintained throughout ongoing arrangements.	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.
4D	Exit strategy	AIs should establish viable exit strategies to ensure that their cloud-dependent operations can continue to run even if a given cloud arrangement is terminated. Exit plans should set out objectives, risk indicators, and detailed procedures for contract termination and migration arrangements, together with clearly defined triggers for initiating an exit. The exit plans should be subject to periodic review and testing to ensure their feasibility and alignment with evolving business requirements.	

9.5 Cloud Security and Data Protection

No.	Domain	Summary of Controls	Tencent Cloud's Response
5B	Secure architecture and deployment	AIs should design and deploy their cloud architecture to be resilient to attacks and unauthorised intrusions. To support this, modern security practices should be embedded across the lifecycle of cloud infrastructure and applications, and include amongst others, effective practices for network design and segmentation, configuration and patch	Customers should design and deploy a cloud architecture that is capable of resisting attacks and unauthorized intrusions. They should also implement effective network design and segmentation, configuration and patch management, securing software and infrastructure, as well as backup and recovery, to ensure the security of the cloud infrastructure and applications. **Network design and segmentation:** **For network segmentation or partitioning**, customers can use **Virtual Private Cloud**

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management, securing software and infrastructure, and backup and recovery. Network design and segmentation • Designing cloud networks with clear segmentation between development, testing, and production environments, and enforcing strict tenant isolation to minimise the risk of cross-environment compromise or lateral attack pathways. Application and API security • Incorporating established secure development disciplines such as systematic threat analysis and adherence to widely recognised application security principles across the entire lifecycle of cloud applications. • Protecting APIs and micro-services through least-privilege access, strong authentication, active monitoring, timely decommissioning of unused interfaces, and safeguards for service discovery and mesh functions. Workload and container security • Applying hardened configurations to virtual machines and containers, limiting unnecessary components, and continuously monitoring for vulnerabilities or misconfigurations.	**(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 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. 1) **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. 2) **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. 3) **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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		• Securing container environments by restricting administrative access to orchestrators, controlling container registries, and allowing deployment only from trusted image sources. • Adopting immutable infrastructure approaches to minimise configuration drift and enable consistent redeployment from version-controlled base images. Automated deployment and configuration management • Leveraging Infrastructure as Code (IaC) and automated Continuous Integration and Continuous Delivery (CI/CD) pipelines to standardise deployments, reduce manual interventions, enforce segregation of duties, and preserve infrastructure integrity. • Deploying Policy as Code tools to automatically validate and enforce compliance with predefined security configurations across cloud components. Cloud security and policy enforcement • Strengthening visibility, threat protection, and policy enforcement across cloud workloads through native security capabilities such as Cloud Access Security Broker (CASB), Cloud-Native	Tencent Cloud has established **network security management standards and a defense-in-depth architecture**. Security domains are defined based on business functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time. **Application and API security:** **In terms of application security development,** Tencent Cloud provides developers with the Cloud Native Build (CNB). CNB, built on the Docker ecosystem, abstracts environments, caches, and plugins, and adopts declarative syntax. Its goal is to help developers build software more efficiently. CNB offers a complete developer tool chain, featuring capabilities such as code hosting, high-performance R&D pipelines, AI code review, cloud-based development environments, artifact management, and customizable task sets. This effectively supports the entire R&D process from requirements to deployment, enabling agile development management. Tencent Cloud has internally established a set of information system security development standards. It actively integrates ISO/IEC 20000 Information Technology Service Management, ISO/IEC 27001 Information Security Management Systems, and ISO/IEC 9001 Quality Management Systems into the entire product security development lifecycle. By incorporating information security and privacy protection principles into different phases—including product requirements, design, development, testing, delivery, and operations—Tencent Cloud ensures that cloud products receive adequate security governance throughout their lifecycle. **Regarding API security**, as the cornerstone of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Application Protection Platform (CNAPP), Cloud Security Posture Management (CSPM), and Cloud Workload Protection Platform (CWPP). Patch management • Implementing a structured patch management process for all cloud resources, clearly defining patching responsibilities between the AI and its CSPs, and ensuring that patches are thoroughly assessed, tested, and deployed in a controlled, phased manner, and are synchronised across production and disaster-recovery environments to prevent inconsistent states or widespread disruption. Backup and recovery • Enforcing technical backup and recovery controls, including timely restoration of critical resources, replication to alternate or recovery sites, and use of segregated or offline systems (e.g. across CSPs, on-premises, or independent storage facilities), to minimise exposure to CSP-level failures. • Conducting regular and scenario-based backup and recovery testing to verify backup integrity, completeness and recoverability, supported by post restoration security validation to ensure recovered environments are hardened before service resumption.	Tencent Cloud's open ecosystem, Cloud APIs cover services provided externally and are continuously iterated. Tencent Cloud APIs support 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. 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. Tencent Cloud offers multiple products to help customers monitor API usage and performance, such as: • **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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			• 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. **Workload and container security:** 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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security services such as DDoS protection, DNS hijacking detection, intrusion detection, vulnerability scanning, web shell detection, and login protection. Tencent Cloud provides customers with the **Tencent Kubernetes Engine (TKE)**, a container-centric, highly scalable, and high-performance container management service built on native Kubernetes. TKE is fully compatible with the native Kubernetes API and extends Kubernetes plugins such as Cloud Block Storage and Load Balancer. It offers a comprehensive suite of features for containerized applications, including efficient deployment, resource scheduling, service discovery, and dynamic scaling, addressing environmental consistency issues across customer development, testing, and operations processes, thereby enhancing the ease of managing large-scale container clusters. In terms of image management, TKE regularly synchronizes official DockerHub images, supports viewing and using DockerHub image repositories, and provides customers with a secure and reliable private image repository, enabling them to create private images. Customers can use **Cloud Access Management (CAM)** to manage access permissions for resources under their accounts. For container image management, **Tencent Cloud Container Registry (TCR)** offers secure, dedicated, high-performance container image hosting and distribution services. Customers can purchase container image service instances in multiple regions worldwide. By setting up custom rules, they can achieve global synchronization of Registry data, meeting the need to pull container images from nearby locations as container services expand globally, and enabling cross-region disaster recovery. Customers can also use **Tencent Cloud Container Security Service (TCSS)** to protect container and image security. TCSS supports

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 virtualization security defence system. **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. **Automated deployment and configuration management:** In terms of automated deployment, customers can leverage Cloud Native Build (CNB), which

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 from coding and building to testing and deployment, delivering both quality and efficiency. 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. **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 operations.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			In addition, 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. **Cloud security and policy enforcement:** Data Security Gateway (Cloud Access Security Broker, CASB) V3.0 is a data protection service designed for applications. It provides data encryption, data masking, and access control capabilities through a configuration-based approach that requires no application development modifications. It supports national cryptographic algorithms and offers field-level data protection on the server side, effectively safeguarding against both internal and external data security threats. In addition, Tencent Cloud provides a one-stop security management platform, Cloud Security Center (CSC), which helps users achieve a closed-loop security operation process—from pre-event threat detection, in-event response and handling, to post-event forensic analysis—through Asset Center, Risk Center, Alert Center, and Advanced Security Management, enabling users to address security issues with a single click. At the same time, Cloud Workload Protection Platform (CWPP) leverages vast threat data accumulated by Tencent's security team and uses machine learning to provide users with security protection services such as asset management, Trojan file detection and removal, hacker intrusion detection, vulnerability risk alerts, and security baseline configuration. It addresses the primary network security risks faced by current servers and helps customers build a robust server security protection system. It now supports unified security protection for servers outside

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud, allowing easy sharing of Tencent Cloud's security intelligence and enabling private data centers to achieve the same level of security experience as on the cloud. **Patch management:** **For Patch Management,** Customers can also leverage **Cloud Workload Protection Platform (CWPP)** to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, issue real-time alerts, and obtain vulnerability remediation solutions, helping them respond rapidly to vulnerability risks. **Tencent Container Security Service (TCSS)** is a virtual patching system developed by Tencent Cloud Security to defend against frequently emerging zero-day vulnerabilities. It integrates Tencent's vulnerability mining and real-time high-risk vulnerability alert technologies to capture and analyze vulnerabilities, generate virtual patches based on Tencent's professional expertise, and automatically enforce these virtual patches on cloud servers, effectively blocking hacker attacks. In addition, customers can use **Vulnerability Scanning Service (VSS)** to conduct regular security scans, continuous risk alerts, and vulnerability detection on the availability, security, and compliance of the enterprise's network devices and application services, and reduce enterprise security risks by following the professional remediation recommendations provided by VSS. Tencent Cloud identifies the latest patches. Tencent Cloud identifies the latest patches and conducts thorough security testing on them prior to installation to ensure the security of patch deployment. Tencent Cloud regularly notifies internal business teams to perform patch upgrades and installations, uses endpoint detection tools to periodically scan patch installation status, and automatically generates alert work orders for devices with overdue

No.	Domain	Summary of Controls	Tencent Cloud's Response
			patches pending installation. **Backup and recovery:** **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 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 6 : How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
5C	Identity and access management	Alongside secure architecture and deployment, AIs should also put in place effective	Customers should establish identity and access control management measures to ensure that only authorized users can access cloud resources

No.	Domain	Summary of Controls	Tencent Cloud's Response
		identity and access management arrangements to ensure that only authorised users and system components can access cloud resources at appropriate privilege levels. Effective arrangements should clearly set out a framework for managing identities, entitlements, and privileges, enforce segregation of duties, promote strong authentication requirements and zero-trust principles, and also apply to both internal and CSP environments. • Defining and documenting cloud IAM roles and responsibilities, including configuration rights, with clear designation of accountable business and technical owners (e.g. application and data owners) for each role. • Maintaining comprehensive IAM policies and procedures for all cloud users and components, with regular reviews and updates, and requiring CSPs, where contracts permit, to support alignment with the AI's IAM provisions, and implementing mitigating controls for any identified gaps. • Enforcing strong authentication for privileged and sensitive cloud access, including multi-factor authentication (MFA) for management consoles and, where relevant, CSP	with the appropriate privilege levels. Customers should also clearly define the requirements for privileged account management, implement the principle of segregation of duties, and enforce strict authentication requirements and the zero-trust principle. **In terms of user account and authorization management**, Cloud Access Management (CAM) enables customers to securely and granularly manage access to Tencent Cloud products and resources. Users can modify sub-user password policies through the CAM console, including password complexity, length, validity period, and other parameters. To prevent password leakage, Tencent Cloud encrypts customer passwords using SHA256 hash algorithm with salt, avoiding the storage of plaintext passwords. CAM also supports multiple forms of secondary identity verification, including MFA device verification or mobile phone verification code, to authenticate identity and ensure environmental security before login and sensitive operations. Additionally, Tencent Cloud supports Single Sign-On (SSO) based on SAML 2.0 and OIDC, allowing external users authenticated via an Identity Provider (IDP) to 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. At the same time, Tencent Zero Trust Security Management is a new-generation office security solution developed based on Tencent's own best practices of building a borderless zero-trust corporate network. Leveraging a zero-trust architecture, it ensures that business resources—both on the cloud and on-premises—remain invisible on the public internet, allowing access only to verified, secure, and trusted users and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		administrative planes or hypervisor access, protected through hardened endpoints, secure protocols, and end-to-end encryption. • Implementing zero-trust principles across cloud environments by enforcing least-privilege access, deny-by-default settings, micro-segmentation, and continuous validation, supported by disciplined access lifecycle management that ensures timely granting, recertification, and revocation of rights at a frequency proportionate to system and data criticality. • Regularly rotating and securing credentials, ensuring the immediate deactivation of unused or expired credentials, and applying secure processes for credential generation, storage and distribution. • Implementing continuous monitoring of user access activities across CSP and internal environments, supported by tamper-resistant audit trails and automated alerting mechanisms to detect unauthorised or anomalous behaviour. • Applying real-time control over privileged activities through granular entitlements, maker-checker functions, and privileged access management (PAM) tools, to prevent unauthorised or high-risk	endpoints. Tencent Cloud has formulated internal access control authorization policies and a separation of privileges matrix mechanism. It requires user accounts to use unique identifiers and sets password policies for employee accounts based on security baselines, including password length, complexity, locking, and reset rules. For internal terminals, operating systems, applications, and network devices, Tencent Cloud has configured policies for login failure limits and session timeouts. Tencent Cloud implements access authentication for employees through a zero-trust security management system, requiring users to complete two-factor authentication (2FA) before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, implementing default minimum privilege control. Employees can only obtain specific permissions through a rigorous approval process when necessary for their work. Tencent Cloud maintains records of employee identity information corresponding to job roles and permission levels across various business systems and conducts regular internal permission audits to prevent privilege abuse or misuse. **For privileged users**, customers can use **CAM** to assign resource permissions to sub-users via tags, achieving granular access control over cloud resources. CAM also supports viewing and tracking employee operation records through **CloudAudit**. Additionally, Tencent Cloud provides **Bastion Host (BH)**, which enables fine-grained authorization based on users, assets, accounts, and operation permissions, ensuring users only have the minimum permissions required to access assets and complete work tasks. Bastion Host also supports operation audit functions, recording and analyzing user operation logs to ensure effective traceability of

No.	Domain	Summary of Controls	Tencent Cloud's Response
		changes. • Adopting federated IAM solutions, where applicable, to unify identities across cloud and other environments (e.g. on-premises environments), and enhancing authentication security through contextual checks such as device, location, and user-behaviour indicators. • Designing IAM architecture for scalability and resilience (e.g. automated account lifecycle management, fault-tolerant and high-availability identity services), supporting secure operations across different cloud deployment models, as applicable.	security incidents. Tencent Cloud has clarified internal management requirements for special access permissions and established relevant authorization mechanisms. Meanwhile, Bastion Host has been fully deployed in Tencent Cloud's production environment to centrally manage administrator account permissions for backend system components. Internal operation and maintenance (O&M) personnel must obtain authorization to access the Bastion Host, with only specific Tencent Cloud O&M staff granted access. Login to the Bastion Host requires two-factor authentication. **Regarding account security monitoring,** CAM grants specific permissions to different personnel for different resources through its granular permission control capabilities. Customers can also view and track employee operation records via CloudAudit, which supports online access to Tencent Cloud console and cloud API operation records within 90 days. Customers data is classified as high-security-level data within Tencent Cloud. Customers have full control over their data, and Tencent Cloud will not attempt to access or disclose customer content. If customers have any questions related to accounts, network security, or product usage, they can submit a work order through the console to obtain technical support. Tencent Cloud provides a comprehensive O&M security guarantee mechanism to ensure that the service team cannot directly access customer information assets without the customer's consent and authorization. Bastion Host service has been fully deployed in Tencent Cloud's production environment. All sensitive operations in the production environment must be performed through real-time login and access via the Bastion Host. Login logs and operation logs are uniformly collected

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and encrypted in Tencent Cloud's log management platform. Logs are audited by automated O&M security audit tools and the internal audit team to detect system or operational anomalies, thereby preventing operational risks.
5D	Data classification and protection	AIs remain ultimately responsible for the security, protection, and integrity of their cloud-hosted data, regardless of the type of cloud arrangements (e.g. outsourced or internally managed) in the process. Accordingly, AIs should systematically classify data based on their sensitivity and business importance, and implement commensurate data protection measures, including layered security controls, as appropriate, across the entire data lifecycle. Areas that should be considered include encryption, cryptographic key management, data loss prevention and secure methods for data disposal. • Classifying data by sensitivity and criticality, with particular attention to confidential business data and customer data, and applying appropriate protection measures such as de-identification, pseudonymisation, or anonymisation where appropriate. • Encrypting data at rest, in transit, in use, and in backup with strong, up-to date cryptographic algorithms and key lengths appropriate to its	Customers should categorize the system based on the sensitivity of the data and the importance of the business, and take corresponding data protection measures, such as data encryption, key management, data leakage prevention, and secure data disposal, to ensure the security, confidentiality and integrity of the cloud-hosted data. To assist customers in complying with regulatory requirements, **regarding data classification and grading,** the Data Security Governance Center (DSGC) can assist customers in automatically organizing data assets, conducting classification, grading, and security risk assessments of enterprise data on the cloud. With the enterprise's authorization, it deeply connects to different types of cloud data assets and obtains real-time data asset information at the kernel level. Based on data characteristics, it helps enterprises identify sensitive data in a targeted manner and sort out data assets from a security perspective. It also assists enterprises in data classification and grading in accordance with national, industry, or enterprise-specific standards. To assist customers in complying with regulatory requirements, Tencent Cloud has established comprehensive internal data classification and grading standards, and all data is uniformly classified and graded in accordance with these standards upon creation. Customer data is classified as high-security-level data within Tencent Cloud. For Tencent Cloud employees, unless the services selected by the customer require processing of customer data, employees

No.	Domain	Summary of Controls	Tencent Cloud's Response
		classification, and regularly reviewing cryptographic standards to address emerging vulnerabilities. • Establishing secure, encrypted channels for migrating and operating servers, applications, and data in cloud environments. • Maintaining comprehensive cryptographic key management policies and procedures, covering justification, secure generation, unique assignment, rotation, backup, deletion, and regular review throughout the key lifecycle. • Exercising independent control over encryption keys, where practicable, through approaches such as Bring Your Own Encryption (BYOE), Bring Your Own Key (BYOK), or Hardware Security Modules (HSMs). Avoiding key reuse across platforms, and ensuring that the encryption key management practices are centralised, scalable, and integrated with IAM processes. • Extending data loss prevention and rights management controls to cloud hosted data, and applying network segmentation and endpoint protection for user devices accessing cloud services. • Regularly evaluating CSP multi-tenancy and logical	will not attempt to access any customer data. **In terms of data storage protection,** multiple Tencent Cloud storage services and database products support data encryption functions, using secure and high-strength encryption algorithms. They implement full-lifecycle key management through integration with the **Key Management Service (KMS)** to ensure data confidentiality. **In terms of data transmission protection,** all communication between customers and the Tencent Cloud console is encrypted and protected by the HTTPS security protocol. The cloud API interfaces and services such as load balancing provided by Tencent Cloud products also feature HTTPS encryption, signature verification, status monitoring, and other security capabilities, providing customers with port-level communication security assurance for their business operations. Furthermore, customers can use the following Tencent Cloud services to achieve secure data transmission in different scenarios: • **Direct Connect (DC)**: Provides dedicated, high-security, and large-bandwidth network connections. Users exclusively occupy the network link, eliminating the risk of data leakage. • **VPN Connection**: Based on network tunneling technology, it enables secure transmission between on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet Key Exchange) and IPsec to encrypt transmitted data, establishing a secure and trusted data tunnel over the public internet to ensure data security during transmission. Additionally, **Data Transfer Service (DTS)** enables synchronization between databases across different deployment types, such as on-premises IDCs, Tencent Cloud, and other third-

No.	Domain	Summary of Controls	Tencent Cloud's Response
		separation controls through technical testing and validation of isolation mechanisms at compute, storage, and network layers, to ensure that tenant-specific protections effectively prevent cross-tenant data exposure. • Ensuring a secure disposal at the end of a data lifecycle by working with CSPs to implement robust data erasure and proper disposal or reuse of hardware and virtual resources, supported by written confirmations and periodic audits, and obtaining final assurance at service exit that all sensitive data have been irreversibly removed with residual risks minimised.	party cloud vendors. Data transmission is achieved via **VPN Connection** and **Direct Connect (DC)**. **In terms of key management,** The Key Management Service (KMS) uses FIPS-140-2 certified Hardware Security Modules (HSMs) to generate and protect keys and supports the full-lifecycle management of customer encryption keys. To reduce the risk of key compromise or abuse, KMS supports key rotation and adopts secure and reliable methods to delete invalid, obsolete, or leaked keys. Deleted keys are irrecoverable, and encrypted data under such keys cannot be decrypted. In addition, Tencent Cloud uses multi-replica redundant storage and erasure coding technology when storing data and immediately takes necessary recovery measures upon detecting integrity errors, greatly improving data fault tolerance. KMS allows customers to use their own key material to encrypt and decrypt sensitive data within Tencent Cloud's architecture, enabling the implementation of a BYOK (Bring Your Own Key) solution on Tencent Cloud. Tencent Cloud has formulated encryption and key management standards, clarifying security requirements for key application, generation, storage, use, transmission, update, destruction, and other processes. All operations involving the key lifecycle implement basic requirements such as dual control, strict handover, proper storage, and timely updates. During key use, requirements such as separation of powers and responsibilities, strict approval, and real-name operations must be followed. Business key operation logs are retained and subject to regular operational audits. In addition, when using cryptographic algorithms for data transmission and storage, Tencent Cloud requires internal teams to comply with international cryptographic management standards or regulations, select high-security-

No.	Domain	Summary of Controls	Tencent Cloud's Response
			level algorithms such as AES-256, and ensure that key lengths meet requirements. **In terms of data access restrictions**, Tencent Cloud provides customers with the **Data Security Audit (DSA)** service. DSA is an AI-based database security auditing system that supports full-volume auditing and storage of various types of session information, access operations, and SQL statements from databases within the enterprise network. It identifies malicious behaviors in operations based on multiple rule libraries and threat detection engines and promptly notifies administrators to take appropriate security protection measures. At the same time, **Tencent Zero Trust Security Management** is a new-generation office security solution developed based on Tencent's own best practices of building a borderless zero-trust corporate network. Leveraging core capabilities such as trusted terminals, trusted identities, trusted applications, and trusted links, it enables terminals to securely, stably, and efficiently access corporate resources and data from any network environment. It monitors the external transmission of sensitive information, supports file auditing and forensics, effectively prevents unauthorized access and leakage of sensitive data, and assists enterprises in intellectual property protection and compliance. Tencent Cloud implements end-to-end identity verification and maintenance for data access permissions across all nodes to ensure the integrity of data assets and the reliability of business services. It has also established real-time monitoring and interception mechanisms to detect and block any abnormal data access behaviors. Furthermore, Tencent Cloud deploys Data Loss Prevention (DLP) tools on employee office terminals to restrict unauthorized data exfiltration, thereby monitoring, detecting, and preventing potential data theft activities. **In terms of tenant isolation**, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			provides security mechanisms such as virtualization control layer resource access control policies, isolation policies between internal private networks on the cloud platform, Web console permission assignment and identity authentication, interface session IDs, and access keys. These mechanisms ensure that each customer can only access the cloud computing resources they have purchased, effectively achieving access isolation between multiple tenants. Through effective isolation methods, it ensures that customer data within the same resource pool remains invisible to each other, and that tenants cannot access, obtain, or tamper with other tenants' data. **For data deletion and destruction**, Tencent Cloud provides a secure and reliable data destruction mechanism. Upon termination of customer services, Tencent Cloud will follow strict data erasure methods to completely delete all customer data, including replicas and backups, after the retention period expires. Deleted data is irrecoverable. When media used to provide Tencent Cloud services malfunctions and needs replacement or reaches the end of its service life and needs to be decommissioned, Tencent Cloud will also promptly clear residual information and conduct thorough physical destruction in accordance with strict processes.
5E	Data residency and regulatory assurance	AIs should ensure that data residency and regulatory obligations are addressed when selecting cloud storage and processing locations, in particular for customer data. This includes maintaining visibility of data locations within CSP infrastructures, assessing cross-boundary transfer risks, and managing subcontracting arrangements to ensure compliance with	Customers should consider data residency and regulatory obligations when choosing cloud storage and processing locations. Additionally, customers should be aware of the data location of the cloud service provider's infrastructure, assess the risks of data crossing borders, and manage subcontracting arrangements, etc. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		applicable laws and regulatory requirements. • Conducting periodic jurisdictional assurance reviews of in-use cloud services to confirm that data storage and processing arrangements remain compliant with evolving data-residency laws and regulatory expectations. This may include monitoring legislative changes in relevant jurisdictions, reassessing cross-boundary data risks, and engaging CSPs to validate that storage or processing locations continue to align with approved regions. • Establishing technical and procedural controls to maintain visibility of actual data locations, such as leveraging CSP-provided location APIs, security dashboards, or data-mapping automation, and validating reported jurisdictions through periodic assurance reviews or third-party audits to evidence compliance with residency restrictions. • Assessing data-related risks arising from subcontracting chains, particularly confidentiality and compliance risks where subcontractors operate in different jurisdictions, including evaluation of the CSP's due-diligence process and transparency regarding subcontractor data-handling or	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 currently operates three data centers in Hong Kong, offering a variety of cloud computing services including cloud servers, cloud databases, and CDN. Hong Kong customers can choose to store and process their data locally within Hong Kong. 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. At the same time, Tencent Cloud provides **Flow Logs (FL)**. After creating a flow log, the system automatically collects log flows from specified scopes (such as cross-region traffic in Cloud Connect Network) and presents the log records in an intuitive and clear manner through dashboards. Tencent Cloud undergoes regular audits by professional third-party auditing bodies each year. 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. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		further transfer arrangements. • Obtaining legal or specialist advice to assess cross-boundary data transfer arrangements, ensuring that mechanisms such as contractual clauses, transfer impact assessments, or approved certification schemes appropriately address applicable data protection and regulatory requirements.	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 HKMA 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.

9.6 Incident Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
6A	Cloud incident management and testing	AIs should ensure that their incident response plans adequately incorporate cloud related risks and dependencies across private, public, hybrid and multi-cloud environments. The plans should clearly set out the actions an AI should take in the event of a disruption involving a CSP.	Customers should formulate an incident response plan, which should cover the risks and dependencies related to the cloud service, and clearly define the actions to be taken in the event of an interruption incident related to the cloud service provider. Additionally, customers should also clarify the escalation, decision-making, and communication coordination strategies with relevant stakeholders. Moreover, customers should regularly review, test, and update the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Amongst others, the plan should set out who bears responsibility for incident escalation, decision-making, communication, as well as coordination with relevant internal and external parties, including CSPs, to support timely investigation, resolution, and regulatory reporting. AIs should also ensure that all legal, regulatory, and contractual reporting obligations relevant to cloud incidents are fulfilled promptly and accurately, with appropriate support and cooperation from CSPs, and that communication with affected stakeholders is transparent and consistent with applicable requirements. AIs should ensure the continued effectiveness of their incident response plans through regular reviews, testing, and timely updates to reflect lessons learned from incidents, system and technology changes, and relevant industry developments.	effectiveness of the incident response plan. To support customers in incident detection and rapid response, Tencent Cloud offers **Cloud Security Center (CSC)**, a one-stop security management platform. With its capabilities including Asset Center, Risk Center, Alert Center, and Advanced Security Management, CSC helps customers establish a closed-loop security operation system covering pre-incident threat detection, in-incident response and handling, and post-incident traceability analysis, thereby enhancing the efficiency of security operations. **In terms of incident management,** Tencent Cloud has formulated internal incident and service request management procedures and established Tencent Cloud incident management policies. These ensure that incidents related to IT service management activities are recorded, classified, prioritized based on impact and urgency, and escalated as needed. This facilitates the prompt resolution and closure of various incidents, minimizes incident impacts, safeguards normal business operations, and improves customer satisfaction. **Regarding incident communication and notification,** Tencent Cloud has developed information security incident management specifications and established relevant procedures for information security incident response, escalation, and notification. These procedures enable timely alerts or notifications to relevant parties—including internal personnel and customers who may be or have been affected by incidents—ensuring orderly, timely, and efficient communication and coordination among all stakeholders. **For security incidents that may affect customers,** Tencent Cloud will, after internal review and based on the scope and severity of the information security incident, notify customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			of the incident handling and analysis results through appropriate channels, and provide corresponding technical support to assist customers in taking remedial measures to minimize losses. **In terms of incident summary and continuous improvement,** Tencent Cloud has established a periodic incident analysis mechanism. It conducts regular multi-dimensional analysis of incidents (including incident type, frequency, impact scope, and severity), and adopts preventive measures based on incident reviews and root cause analysis to prevent recurrence of similar incidents. For major security incidents, Tencent Cloud will set up a dedicated task force to prepare a special analysis report and submit it to the management. **For customers to report issues or take the initiative to contact Tencent Cloud,** the Tencent Cloud official website console provides a work order service, supporting customers in reporting faults, incidents, problems, and complaints related to security, availability, and confidentiality. The Tencent Cloud order system assigns priorities to customer work orders through a tiered response mechanism. When the first-line technical team is unable to resolve the issue effectively, the system will automatically trigger a service escalation process, with product or technical teams intervening to collaborate on resolution, ensuring that customer needs or feedback receive timely responses and handling. In addition, Tencent Cloud provides online and telephone channels on its official website to support customers in reporting problems encountered while using Tencent Cloud services. Tencent Cloud has multi-region mutually backup customer service centers, capable of handling customer inquiries and needs 24/7 uninterruptedly, and providing high-quality round-the-clock technical support.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers may also select applicable service plans to obtain exclusive support, including dedicated support groups, dedicated technical account managers, and value-added services.

9.7 Ongoing Monitoring

No.	Domain	Summary of Controls	Tencent Cloud's Response
7A	Integrated security monitoring	AIs should conduct ongoing monitoring of their CSP arrangements to ensure that any security compromises are detected in a timely manner. Accordingly, AIs should implement integrated security monitoring across their cloud environments, consolidating data from multiple sources to support timely alerts, centralised visibility, and proactive detection of security threats and other cloud-related anomalies. Monitoring should, where feasible, cover key security and operational layers and extend to CSPs and their subcontractors. Security operations centre (SOC) strategies should make use of monitoring data made available by CSPs and, where possible, subcontractors, in combination with the AI's own data, to enable comprehensive analysis and timely escalation and response to detected events. Monitoring capabilities should be regularly evaluated and optimised to ensure alerts remain reliable, actionable, and effectively integrated into the	Customers should implement security monitoring for their cloud environment, integrating data from multiple sources, actively detecting and promptly identifying security threats and abnormal situations related to the cloud. Customers should combine the monitoring data provided by the cloud service provider and its subcontractors with their own data for comprehensive analysis and promptly report and respond to the detected incidents. In addition, customers should regularly optimize and evaluate the monitoring strategies. 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. Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		AI's incident response processes.	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. To meet regulatory requirements for multi-source data integration, centralized visualization, and comprehensive monitoring spanning security and operational layers, and to support customers in building integrated security operation capabilities, Tencent Cloud provides a unified and robust foundation for aggregating and collecting multi-source data. This serves as a primary data source for customer SOC analysis, alert correlation, and incident response: • **CloudAudit**: Records logs of all cloud resource operations, fulfilling the need for traceability auditing and accountability verification. • **Cloud Log Service (CLS)**: Provides standardized log storage and retrieval, supporting full-dimensional collection of VPC flow logs, object storage access logs, container logs, etc.; • **Cloud Monitor (CM)**: Achieves 20+ types of cloud resource performance and availability monitoring in seconds, covering key operational aspects such as computing, network, storage, and databases. The data sources available on Tencent Cloud can be uniformly exported to customers' existing security systems, enabling seamless integration with customer-owned data for holistic analysis, rapid alerting, and timely incident handling. This supports periodic evaluation and optimization of monitoring capabilities, aligning with requirements for in-depth monitoring of cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			environments and closed-loop incident response.
7B	Service performance and log management	Ongoing monitoring should extend to service performance and log management too. For service performance, AIs are expected to monitor compliance with SLAs, contractual obligations, and regulatory requirements, with particular attention paid to critical or important outsourced functions. This includes monitoring availability, reliability, and auditability, supported, where appropriate, by independent validation tools, and maintaining awareness of CSP service updates and lifecycle events to enable timely risk assessment and mitigation. For log management, AIs should establish cloud-specific approaches that ensure the completeness, integrity, and availability of log data across relevant systems and services. Logs should provide reliable visibility into user and system activities, including privileged or administrative operations where applicable, to support timely detection, investigation, and audit of cloud-related events in accordance with regulatory and institutional requirements.	Customers should monitor the service performance, compliance status, and contract fulfillment of the cloud service provider in accordance with the service level agreement signed. In addition, customers should record logs related to users and system activities and ensure the security of the logs to support the detection, investigation, and review of cloud-related incidents. **For the service performance**, Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. **To assist customers in log collection, aggregation, and analysis,** Tencent Cloud provides **Cloud Log Service (CLS)**. As a one-stop log management platform, CLS offers a full range of services from log collection and storage to log search and analysis, real-time consumption, and log delivery, helping customers address needs related to business operations, security monitoring, log auditing, and log analysis. CLS adopts a highly available distributed architecture, storing log data with multi-redundancy backups to prevent service unavailability due to single-node failures, ensuring high service availability and providing stable and reliable support for log data. **Cloud Security Center (CSC)** also supports collecting various cloud security-related data, including

No.	Domain	Summary of Controls	Tencent Cloud's Response
			alerts from cloud security products, cloud asset configuration change data, cloud user operation behavior data, and logs from selected cloud products. It provides a unified search and investigation platform to enable customers to conduct comprehensive cloud log auditing, search, and investigation. Additionally, Elasticsearch Service (ES) aggregates and transmits real-time logs from cloud servers, containers, and other cloud products, as well as historical and incremental business data, to Tencent Cloud ES clusters for distributed data storage, query, and analysis. **For the collection and retention of network logs**, Cloud Firewall (CFW) supports full-traffic network log analysis with a maximum retention period of 6 months. It also provides advanced threat traceability analysis, enabling the analysis of domain name registration, resolution, filing, and historical resolution information. **For the collection and retention of operation logs,** customers can use CloudAudit to conduct supervision, compliance checks, operation reviews, and risk audits of Tencent Cloud account activities. CloudAudit supports online access to Tencent Cloud console and cloud API operation records within 90 days. To assist customers in complying with regulatory requirements, Tencent Cloud has established log collection and management specifications and mechanisms for logs such as login logs, operation logs, system regular logs, and system security event logs. These mechanisms govern the recording, extraction, storage, protection, analysis, and auditing of logs to detect and prevent abnormal system activities and risks. Logs are uniformly collected and managed in Tencent Cloud's log management platform, with backup and strict protection measures implemented to prevent unauthorized modification or deletion. Tencent Cloud audits

No.	Domain	Summary of Controls	Tencent Cloud's Response
			logs through automated O&M security audit tools and internal audit teams to detect system or operational anomalies, thereby mitigating operational risks.

9.8 Workforce Strategy and Empowerment

No.	Domain	Summary of Controls	Tencent Cloud's Response
8A	Workforce strategy and resource management	AIs should maintain adequate in-house competencies and resources at all levels, from the Board, senior management, and staff across the three lines of defence, to carry out effective oversight and operations of cloud computing arrangements. To support this, the Board and senior management should have sufficient technical and managerial knowledge to understand the risks and implications, while operational teams should have the expertise to implement and sustain cloud strategies. Workforce planning should also be responsive and adaptive to the AI's evolving cloud journey. Engagement of external expertise should be strategic and well controlled, complementing internal capabilities rather than substituting an AI's accountability in managing critical cloud functions.	Customers should ensure that all levels of internal personnel possess sufficient professional capabilities and resources. For instance, the management should have adequate technical and management knowledge to understand the risks and impacts related to the cloud; the operational staff should have the professional skills to implement and maintain cloud technologies. In cases where internal capabilities are insufficient, external experts can be employed to supplement the internal capacity. Tencent Cloud has established organizational frameworks related to cloud security and information security, clarified security function roles and corresponding responsibilities at different levels, and defined working mechanisms such as information security auditing and information security risk assessment. Tencent Cloud has set up a Security Technology Committee and specialized security teams across various functions and domains, and assembled a team of senior industry experts, committed to providing customers with secure, reliable, professional and compliant products and services. Tencent Cloud has also defined the composition of information security liaisons; these regional information security liaisons maintain smooth communication with local regulatory authorities and customers in accordance with compliance and business requirements to ensure that Tencent Cloud adheres to legislation, regulatory provisions and contractual agreements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers should formulate a structured training plan tailored for different positions, to ensure that employees can effectively supervise cloud business and ensure operational work. Additionally, customers should also provide regular training covering the core elements of cloud management.
8B	Workforce training and competency development	To operationalise and sustain the workforce strategy, structured and role-specific training programmes should be established to ensure that the Board, senior management, and staff across the three lines of defence maintain up-to-date knowledge and skills for effective cloud oversight and resilient operations. To achieve this, training should be provided on a regular basis and should address core dimensions of cloud management. These programmes should be continually updated to reflect the latest developments in cloud technology, regulatory expectations and operational needs.	Tencent Cloud has formulated a comprehensive internal human resource (HR) security management standard, including verification of competence and qualifications of employees prior to onboarding, and on-the-job skills training after onboarding. Tencent Cloud has also established a robust internal information security training mechanism, requiring regular employees, consultants, interns, and contract employees to complete information security training courses. These training courses include mandatory training for all staff, specialized training for key positions, and optional professional courses covering areas such as basic security awareness, office security, vulnerability identification and defense, privacy protection, emergency response, R&D security specifications, and data security requirements. Operational procedures, user manuals, and other documentation for Tencent Cloud's products have been formalized and made available to customers through the official website. Tencent Cloud also provides customers with training and certification based on Tencent Cloud product knowledge and relevant professional competencies to enhance their technical capabilities and cloud proficiency.

10

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guideline on Authorization of Digital Banks

"Digital banking" refers to banks that provide banking services entirely or primarily through the Internet or other forms of electronic channels. The Hong Kong Monetary Authority (HKMA) welcomes institutions to establish digital banks in Hong Kong and believes that the development of digital banking will promote the application and innovation of financial technology in Hong Kong, offering new experiences to banking customers.

The Guideline on Authorization of Digital Banks sets out the principles considered by the Monetary Authority when deciding whether to grant authorization for a digital bank to conduct banking business in Hong Kong. It requires digital banks to comply with the same set of regulatory requirements applicable to traditional banks, with other requirements adjusted using a risk-based and technology-neutral approach to accommodate the digital banking business model.

This section summarizes the control requirements related to technology risk and outsourcing in the Guideline on Authorization of Digital Banks that are relevant to cloud service providers, and explains how Tencent Cloud, as a cloud service provider, assists AIs in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers should pay attention to technology-related risks and adopt appropriate control measures, particularly in the areas of information security, system resilience, and business continuity management.
14	Technology risk - Information Security	Technology related risk, especially information security, system resilience and business continuity management, is of vital importance to a digital bank. Security breaches and unauthorized tampering with the systems of the bank could result in financial loss as well as loss of reputation. The general principle is that the security and technology related controls in place should be "fit for purpose", i.e. appropriate to the type of transactions which the digital bank intends to carry out.	**In terms of information security,** Tencent Cloud has established information security management policies to support the secure operation and risk management of the cloud platform. Through advanced cloud computing technology, network security protection capabilities, global data center deployment, and industry solutions, Tencent Cloud provides security protection for the entire data lifecycle and a secure, reliable cloud computing environment. For more information on information security, please refer to Section 5.2 "Security Management" and Section 10: How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guideline on Customer Data Protection. **In terms of system resilience and business continuity,** Tencent Cloud is certified under the ISO/IEC 22301 international standard for business continuity management. To ensure service availability, Tencent Cloud has developed detailed disaster recovery plans for its products and services and conducts regular drills to validate timeliness

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and feasibility. For more information related to system resilience and business continuity, please refer to Section 6: How Tencent Cloud Meets and Assists Customers to Meet the Requirements of TM-G-2 Business Continuity Planning.
15	Technology risk - Independent Assessment	In this connection, a digital bank applicant will be required to engage a qualified and independent expert to perform an independent assessment of the adequacy of its planned IT governance and systems. A copy of this assessment report should be provided to the MA as part of the documents submitted on application. A more detailed independent assessment of the actual design, implementation and effectiveness of its computer hardware, systems, security, procedures and controls should be undertaken and the report of the assessment should be provided to the MA before the digital bank commences operation. The bank should also establish procedures for regular review of its security and technology related arrangements to ensure that such arrangements remain appropriate having regard to the continuing developments in technology.	Customers should conduct a detailed independent assessment of their IT governance, systems, hardware, security, procedures, and control measures, and submit an independent assessment report to regulators as required. To support customers' assessment needs, Tencent Cloud will, based on actual circumstances and agreements with the customer, cooperate with third-party security audits and supervision, provide dedicated personnel assistance, and actively respond to customer-initiated audit activities. Tencent Cloud security team performs 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 third-party audits and provides assurance-based System and Organization Controls (SOC) reports, disclosing the latest internal control status of Tencent Cloud's service organization to cloud customers, independent auditors, regulators, shareholders, and other stakeholders.
23	Outsourcing	The MA does not object in principle to outsourcing of computer or business operations of a digital bank to a third party service provider, which may or may not be part of the group owning the digital bank. Digital banks should discuss their plans for material outsourcing with the	Customers should comply with relevant requirements under regulatory provisions such as SA-2 Outsourcing Guidelines and the Personal Data (Privacy) Ordinance and implement adequate security and control measures for outsourcing activities to ensure the confidentiality and integrity of customer information and safeguard regulatory oversight rights. **Tencent Cloud designs and builds its cloud**

No.	Domain	Summary of Controls	Tencent Cloud's Response
		MA in advance. They should demonstrate that the principles in the SPM module on "Outsourcing" (SA-2) will be complied with. In particular, the MA must be satisfied that the operations outsourced remain subject to adequate security controls, that confidentiality and integrity of customer information will not be compromised and that the requirements under the Personal Data (Privacy) Ordinance and common law customer confidentiality are complied with. The MA should have the right to carry out inspections of the security arrangements and other controls in place 5 in the service provider or to obtain reports from a relevant supervisory authority, external auditors or other experts. The MA must also be satisfied that his powers and duties under the Ordinance will not be hindered by the outsourcing arrangements.	**services in accordance with internationally recognized information security and IT governance standards**, strictly adheres to applicable laws and regulations in the jurisdictions where it operates, and has established security compliance procedures to ensure that information security operations meet relevant legal, regulatory, and standard requirements. Tencent Cloud has obtained multiple internationally recognized security and compliance certifications, providing customers with cloud products and services verified by authoritative third-party certification bodies. **As a cloud service provider, Tencent Cloud actively supports customers' outsourcing management requirements**, including providing and signing relevant service agreements based on actual customer needs, responding to and cooperating with audits or assessments initiated by customers or their regulators, and offering a variety of security protection measures and related cloud products/services to ensure the confidentiality and integrity of customer data on the cloud. For more information related to outsourcing, please refer to Section 7 : How Tencent Cloud Meets and Assists Customers to Meet the Requirements of SA-2 Outsourcing and Guidance on Cloud Computing."

11 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Customer Data Protection



Customer Data Protection, updated in 2014, aims to remind authorized institutions of the importance of safeguarding the confidentiality of customer data and provides guidance on key control measures to prevent and detect any loss or leakage of customer data. The provisions related to cloud service providers mainly focus on areas such as data security policies and awareness, logical access control for customer data, customer data storage management, physical security controls related to customer data, and controls over service providers.

In this section, Tencent Cloud summarizes the control requirements in the Customer Data Protection guideline that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists authorized institutions in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
B	Data security policies and awareness	AIs should develop formal policies and procedures on data security to safeguard customer data, covering areas on, among others, system controls, physical security controls, mobile computing, and outside service providers. The policies and procedures should be in line with the relevant supervisory guidance issued by the HKMA from time to time. Where personal data are involved, the policies and procedures, including those to be followed by the relevant service providers, should also be in line with PDPO and any relevant codes of practice, rules or guidance issued or approved by the Privacy Commissioner. Moreover, AIs should formulate an effective awareness programme reminding staff at least annually of the importance of complying with the data security policies and procedures, prompt reporting of potential leakage or loss of customer data and the possible disciplinary actions for any violations.	Customers should establish data security policies and procedures in compliance with HKMA regulatory guidelines and the Personal Data (Privacy) Ordinance, covering areas such as system controls, physical security controls, mobile computing, and external service providers. Customers should also implement awareness programs to enhance employees' understanding of data protection. **To support customers in meeting regulatory requirements, Tencent Cloud has established a comprehensive information security and privacy protection management system**, strictly adhering to cybersecurity, user privacy, and data security laws and regulations in the jurisdictions where it operates. Tencent Cloud regularly reviews its information security policies to ensure that the objectives and controls of its cloud security system comply with relevant security strategies, standards, procedures, and legal requirements, ensuring the adequacy and effectiveness of its policies. Based on this, Tencent Cloud has built a multi-layered security framework using a "one center, three lines of defense" model. While ensuring the security of the underlying cloud platform, Tencent Cloud empowers customers by providing a wide range of cloud security features, tools, and controls, working together to build a more robust security assurance system in the cloud. **In terms of employee awareness training**, Tencent conducts diversified programs, including but not limited to offline and online courses,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			internal sharing sessions, and micro-learning updates, to communicate the company's personal information and privacy protection policies, processes, and standards through multiple channels. These programs ensure employees understand their responsibilities for data and privacy protection, the potential disciplinary consequences of non-compliance, and acquire the necessary skills to implement data protection effectively.
C	Logical access controls of customer data	AIs should identify the locations of customer data residing in different parts of AIs' networks and systems and ensure that adequate logical access controls are in place at different levels (e.g. application level, database level, operating system level, network level) to prevent unauthorized access to customer data and unauthorized/erroneous transmission of customer data to external parties. These controls should include: • the rights to access customer data and transmit customer data to external parties should be granted on a need-to-have basis only; • the tools for massive download of customer data can be used only upon proper approval from the management and the use should be promptly revoked if the approval is no longer valid; • proper re-certification of user access and access rights should be performed at least annually (more	Customers should identify customer data residing in different parts of their networks and systems and ensure that adequate logical access controls are implemented at various levels to prevent unauthorized access or transmission. **To assist customers in meeting regulatory requirements for access control,** Tencent Cloud provides **Cloud Access Management (CAM)**, which enables secure and granular management of access to Tencent Cloud products and resources, and integrates with **CloudAudit** for tracking and auditing employee operations. Tencent Cloud adheres to the principle of 'data privacy' by implementing multi-layered technical isolation measures to ensure tenant data is mutually invisible, thereby preventing tenants from accessing, obtaining, or tampering with other tenants' data. Internally, Tencent Cloud has established access control management standards and deployed bastion hosts across production environments, allowing only authorized internal operations personnel to log in and perform actions through secondary identity verification. Tencent Cloud also maintains records of personnel identity information and corresponding role-based permissions for all business systems and conducts regular internal permission reviews to prevent misuse or abuse of access rights. **For secure remote access**, customers can use **VPN Connection** to establish encrypted transmission between their on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet

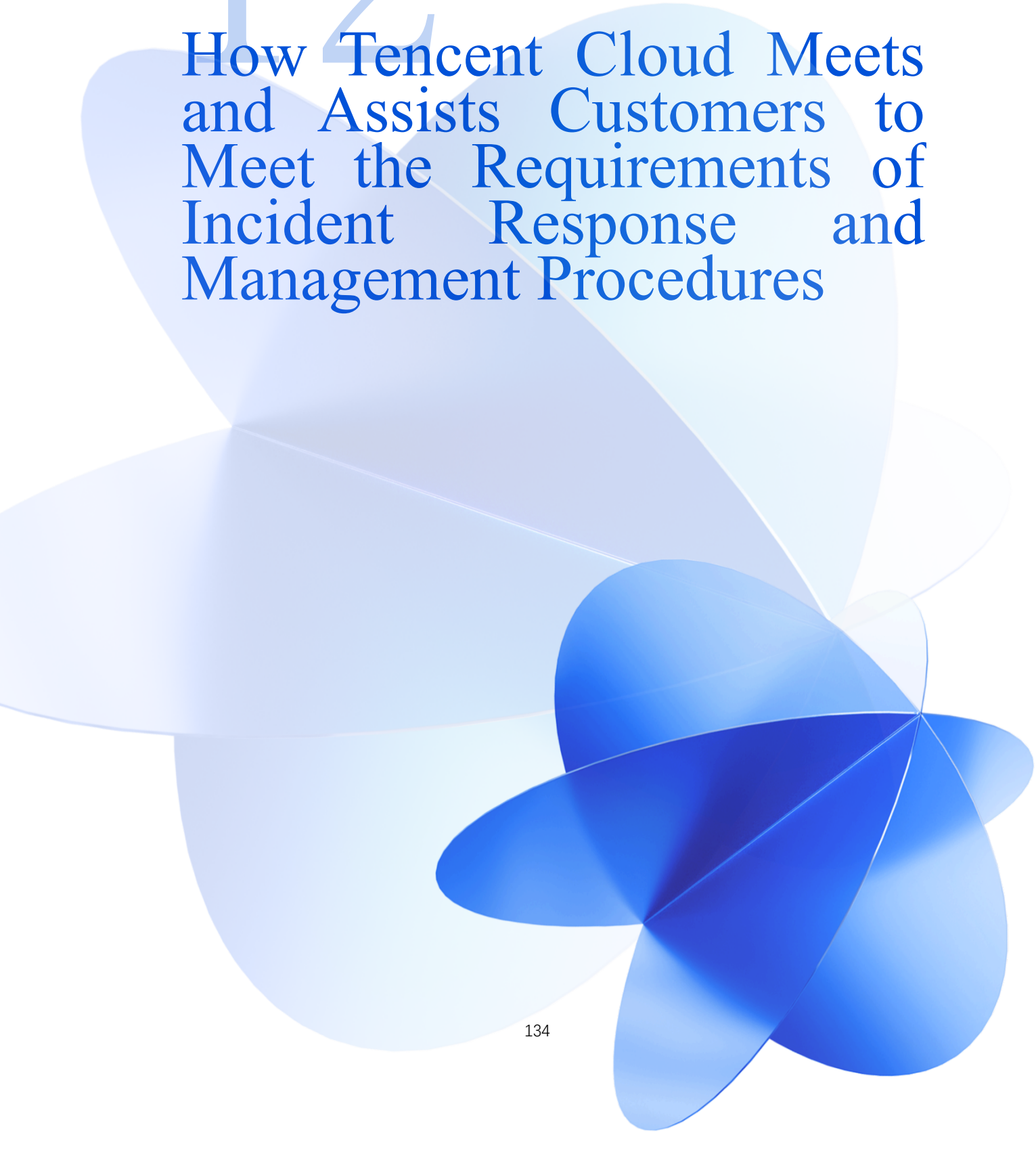
No.	Domain	Summary of Controls	Tencent Cloud's Response
		frequently for systems or user access rights of higher risk or sensitivity); • audit trail should be enabled whenever there is a need for detection of unusual activities • regular reviews of audit trails should be conducted, supported by effective follow-up actions; • system and network infrastructure with robust security controls; • remote access by AIs' staff or service providers from external networks (including from the Internet) to the customer data stored in the AIs' or service providers' systems should be subject to robust authentication (e.g. two-factor authentication) and the data being transmitted should be subject to strong data encryption.	Key Exchange) and IPsec protocols to encrypt data in transit, creating a secure and trusted channel over the Internet. The VPN gateway offers high reliability with an underlying dual-machine hot standby architecture to ensure uninterrupted communication sessions and seamless application experience. Tencent Cloud also supports SSL VPN technology for secure and fast remote access to cloud business systems, protecting data transmitted over the Internet through encryption. **For system and network infrastructure security,** Tencent Cloud provides mature network security architecture with multiple protection mechanisms, including firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS protection, network segmentation, and web application security, to promptly detect, filter, and block malicious traffic and safeguard Tencent Cloud's network. Tencent Cloud has also established network security configuration standards and baseline requirements to standardize security settings for network devices and operating systems of host servers. Tencent Cloud regularly reviews security policies and parameter configurations for routers, firewalls, and network servers to ensure their effectiveness. Additionally, Tencent Cloud operates an internal network monitoring system for real-time monitoring and alerting network devices and deploys Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints across the network. For more information on access control, system, and network infrastructure, please refer to Section 5.2 'Security Management' and Section 5.5 'Communication Network'.
E	Controls over storage of customer data	AIs should take effective measures to mitigate the risk of unauthorized downloading of customer data to portable storage media (e.g., USB drives) and the loss of such media containing	Customers should implement effective controls to manage activities such as downloading customer data to portable storage media, promptly detect and address abnormal download activities that may involve customer data, and establish secure processes for the destruction of data stored on such

No.	Domain	Summary of Controls	Tencent Cloud's Response
		customer data. AIs should implement effective controls to promptly detect unusual downloading activities that may involve customer data and take appropriate and timely follow-up actions to confirm whether such activities constitute unauthorized leakage of customer data. For all media (including paper and electronic media) where customer data is stored, AIs should establish secure processes for disposal and destruction of customer data stored in such media, in line with section 3.1 on information classification and protection of the SPM module on 'General Principles for Technology Risk Management.'	media. **To assist customers in detecting and controlling abnormal data-related activities**, Tencent Cloud provides Cloud Data Security (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 within Tencent Cloud is classified at the highest security level. Except when required for service delivery or troubleshooting and with explicit customer authorization, or under investigation by national or local government authorities in accordance with applicable laws, Tencent Cloud employees will never proactively access any customer data. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability and has established real-time monitoring and interception mechanisms to detect and block abnormal data access activities. Additionally, Tencent Cloud deploys a zero-trust security management system on employee computers to monitor and restrict the external export of sensitive data. **For the disposal and destruction of sensitive information**, Tencent Cloud provides secure and reliable data erasure mechanisms. When a customer's cloud service is terminated, Tencent Cloud follows strict data wiping procedures permanently deleting customer data—including copies and backups—after the retention period expires, ensuring that deleted data cannot be recovered. When media used to deliver Tencent Cloud services fail and require replacement or reach end-of-life, Tencent Cloud promptly performs complete physical destruction in

No.	Domain	Summary of Controls	Tencent Cloud's Response
			accordance with rigorous processes.
G	Physical security controls over and office environment related to customer data	AIs should identify the locations within and outside their premises (including service providers) where customer data are stored or can be accessed. They should ensure that adequate physical security measures (including physical access controls, security guards, and surveillance cameras) are in place at these locations to safeguard customer data against theft or unauthorized access. When AIs or their service providers (e.g., couriers) need to relocate or transport systems, facilities, records, or other assets containing customer data, they should arrange adequate physical security controls to protect these assets and data during relocation or transportation. Appropriate reconciliation or inventory checks should be performed as soon as practicable during and after the relocation or transportation to ensure that no customer data are lost in transit. AIs should implement controls over their premises or service providers that process or have access to large quantities of sensitive customer data to reduce the risk of customer data theft.	Customers should identify locations within and outside their premises (including service providers) where customer data is stored or can be accessed and establish adequate physical security measures. To assist customers in meeting regulatory requirements, Tencent Cloud has implemented a physical security management framework to standardize operational safety, promptly identify risks, and strengthen physical security controls. **For physical access control**, Tencent Cloud data centers enforce strict infrastructure and environmental access controls based on different security levels for designated zones. All visitors and staff entering data centers must undergo identity verification and inspection of personal belongings, with items duly registered. Tencent Cloud maintains a comprehensive personnel access control matrix within its data center access authorization system, based on personnel categories and access privileges, to effectively manage access and operational activities. In addition, Tencent Cloud's financial zone data halls use dedicated cages to physically isolate equipment belonging to different customers and are equipped with biometric access systems to prevent unauthorized personnel from accessing customer equipment. **For security and monitoring**, Tencent Cloud data centers deploy security personnel who conduct inspections of server rooms and equipment strictly according to checklists and schedules, signing and recording inspection times at each checkpoint. Any infrastructure failure or security incident triggers the data center emergency response process immediately. Furthermore, Tencent Cloud data centers are equipped with 24/7 video surveillance systems with full coverage and alerting capabilities,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			monitored from security control rooms, with recordings securely stored and retained for an adequate period.
I	Other controls over service providers	For outsourcing arrangements that involve storage of and/or access to AIs' customer data, AIs should require their outsourcing operators and other service providers that store, transport or have access to customer data to comply with the AIs' data security policies and procedures including the controls set out in this document. AIs should implement effective controls to monitor and validate the service providers' compliance situation. Such requirements should be specified clearly in the agreements and AIs should conduct a regular assessment to ensure that the service providers comply with all relevant requirements. In addition to the controls set out above, where there is an operational need for AIs to transmit customer data to their service providers over public network, strong data encryption should be in place to protect the customer data during transmission	Customers should implement effective measures to ensure that service providers comply with their data security policies and procedures and should monitor and verify the compliance status of service providers. If customer data needs to be transmitted to service providers over public networks, strong encryption measures should be implemented to ensure transmission security. To assist customers in meeting regulatory requirements, Tencent Cloud actively supports customers' outsourcing management needs by clearly defining, in online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure matters. Tencent Cloud can also provide dedicated personnel to assist and cooperate with audits or assessments initiated by customers. For data transmission security in Internet environments, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud products also provide cloud API interfaces with security capabilities such as HTTPS encryption, signature verification, and status monitoring. Customers can further enhance transmission security by using services such as **Direct Connect (DC)** and **VPN Connection**.

12 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Incident Response and Management Procedures



The Incident Contingency and Management Procedures reminds AIs of the need to maintain effective contingency, management capabilities, and procedures for major incidents. It also sets out principles that AIs should follow when making public disclosures about such incidents. The relevant requirements mainly focus on areas such as rapid incident response, notifying affected customers, issuing public announcements for major incidents, reporting significant events to the HKMA, handling inquiries from customers and media during major incidents, and enhancing detection and response capabilities for major incidents.

As a cloud service provider, Tencent Cloud supports AIs in meeting these regulatory requirements by focusing on robust incident detection and response capabilities, as well as communication strategies and notification procedures.

12.1 Incident Detection and Rapid Response

The guideline requires AIs to have appropriate incident response and management capabilities to promptly analyze the root cause of incidents and quickly correct or contain issues to protect the interests of customers who are or may be affected.

To help customers detect and respond to incidents quickly, 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, enabling customers to achieve a closed-loop security operation covering pre-incident threat detection, in-incident response, and post-incident forensic analysis, thereby improving operational efficiency.

Internally, Tencent Cloud has established an Information Security Incident Management Standard, including reporting, response, and handling mechanisms and processes. Security incidents are recorded in Tencent Cloud's internal security operations system. Detected incidents are analyzed and classified based on factors such as nature, data sensitivity, and impact scope, and promptly escalated to responsible personnel for follow-up.

Tencent Cloud is committed to building a proactive defense capability framework of "Intelligence–Defense–Management–Planning," leveraging threat intelligence, AI, and big data technologies to enhance incident response efficiency. Supported by a 24/7 security operations system, Tencent Cloud's security team focuses on vulnerability monitoring, intrusion tracing, and attack blocking, responding to alerts in real time and quickly formulating emergency response plans to contain incident spread. For major security incidents, Tencent Cloud forms a dedicated task force to produce detailed analysis reports for senior management.

12.2 Communication Strategy and Notification Procedure

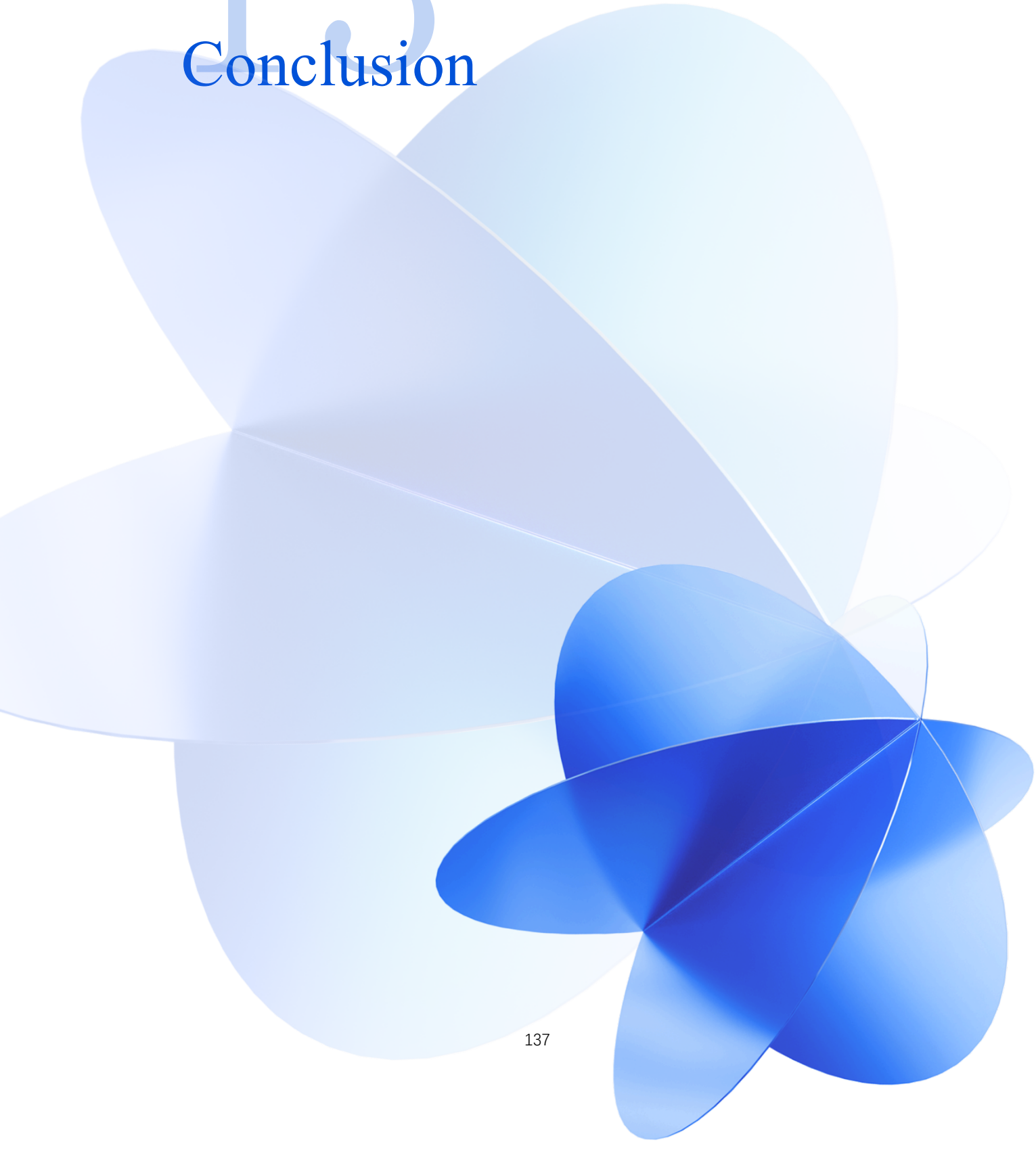
Under regulatory requirements, AIs should promptly assess the impact of an incident upon discovery and proactively notify affected or potentially affected customers and other impacted AIs through effective channels. AIs should also establish communication strategies to ensure that, in the event of a serious incident or one affecting many customers, the HKMA is notified immediately, consistent and up-to-date information is conveyed to stakeholders, and public announcements are considered.

To support customers in fulfilling communication and notification obligations, Tencent Cloud has implemented an Information Security Incident Communication and Early Warning Management Procedure, establishing clear warning and notification mechanisms for significant security incidents and major business disruption scenarios, and promptly inform and alert affected internal personnel, customers, and other relevant parties, ensuring orderly, timely, and efficient communication and coordination.

For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels and provide technical support to help minimize losses.

To assist customers in reporting issues or contacting Tencent Cloud proactively, Tencent Cloud offers a ticketing service via its official console, enabling customers to report faults, incidents, 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 if frontline support cannot resolve the issue, ensuring timely handling. Tencent Cloud also provides online and telephone channels on its official website for customer feedback. With geographically redundant customer service centers operating 24/7, Tencent Cloud delivers high-quality, round-the-clock technical support. Customers can choose service plans that include dedicated support groups, technical account managers, and value-added services for tailored assistance.

13 Conclusion



Tencent Cloud is the cloud computing brand developed by Tencent Group, leveraging years of technological expertise and security practices. Tencent Cloud is committed to continuously providing customers with a secure, reliable, and intelligent cloud platform, empowering more enterprises to efficiently embrace digital transformation and drive secure business growth.

This guide is based on key regulatory requirements from Hong Kong Monetary Authority (HKMA) and aims to provide customers with a comprehensive and transparent overview of how Tencent Cloud supports compliance for systems and data hosted in the cloud. It is designed to help enterprise customers confidently and securely migrate their systems and data to the cloud.

Through this guide, Tencent Cloud hopes to assist enterprise customers in effectively meeting HKMA compliance standards, while also achieving efficient digital upgrades and innovative business development.

This guide is for reference only. Customers are advised to consider their own specific circumstances when using the information provided, to ensure regulatory compliance during their use of Tencent Cloud services.

14 Version History



Date	Version	Detail
April 2026	V1.0	Initial Release