



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

April 2026

Copyright Notice

©2013-2026 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

This document is 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 BNM Requirements of Outsourcing	
06	How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Management of Customer Information and Permitted Disclosures	
6.1	Control environment	35
6.2	Customer information breaches	54
6.3	Outsourced service provider	58
07	How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Data Management and MIS Frameworks	
08	How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Business Continuity Management	
09	How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Risk Management in Technology ("RMiT")	
9.1	Technology Operations Management	94
9.2	Cybersecurity Management	122
9.3	Technology Audits	127
9.4	External Party Assurance	129
9.5	Security Awareness and Training	130
9.6	Consultation and Notification related to Cloud Services and Emerging Technology	131
9.7	Control Measures on Cybersecurity.....	132
9.8	Key Risks and Control Measures for Cloud Services	144
9.8.1	Cloud Governance	144
9.8.2	Cloud Design and Control.....	150
10	How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of	

CONTENTS

Electronic Know-Your-Customer ("e-KYC")

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

11.1 Governance	178
11.2 Technology Risk Management.....	180
11.3 Technology Operations Management	182
11.4 Technology Service Provider Management	211
11.5 Cybersecurity Management	224
11.6 Guiding Principles Relating to The Adoption of Artificial Intelligence (AI) and Machine Learning (ML)	238

12 How Tencent Cloud Meets and Assists Customers to Meet the SC Requirements of Guiding Principles on Business Continuity

13 Conclusion

14 Version History

01

Overview

Against the backdrop of in-depth global integration, accelerated technological iteration, and diversified financing needs, Malaysia's financial landscape has undergone remarkable transformation, driving financial institutions to continuously deepen the application of digital technologies for enhanced service efficiency. However, digital transformation has also exposed financial institutions to more complex technology-related risks, such as customer information leakage and business disruptions, which pose potential challenges to financial security.

To regulate the technology application practices of financial institutions and strengthen risk management and control, Bank Negara Malaysia (hereinafter referred to as "BNM") and the Securities Commission Malaysia (hereinafter referred to as "SC") have formulated and issued a series of regulatory policies. These policies focus on core domains including outsourcing services, technology risk management, business continuity management, and customer information management. They provide clear compliance guidelines for financial institutions, safeguard the security and stability of technology applications, and promote the orderly advancement of digital transformation in the financial sector.

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

Bank Negara Malaysia (BNM):

- [Outsourcing](#)
- [Management of Customer Information and Permitted Disclosures](#)
- [Guidelines on Data Management and Management Information System \("MIS"\) Framework for Development Financial Institutions \("DFI"\)](#)
- [Business Continuity Management](#)
- [Risk Management in Technology \("RMiT"\)](#)
- [Electronic Know-Your-Customer \("e-KYC"\)](#)

The Securities Commission Malaysia (SC):

- [Guidelines on Technology Risk Management](#)
- [Guiding Principles on Business Continuity](#)

02

Tencent Cloud Security and Privacy Compliance

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

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

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

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

2.1 Global Compliance

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

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

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

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

2.2 ISO/IEC Certification

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

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

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

2.3 Regional and Industry Compliance

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

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

in Malaysia

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

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

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

03

Tencent Cloud Security Responsibility Sharing Model

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

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

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

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

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

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

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

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

04

Tencent Cloud Global Infrastructure

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

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

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

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

05

How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing

Increasing digitalisation and advancement in financial technologies have further spurred financial institutions to continuously adapt their business models and processes through outsourcing, which is increasingly used as a means of improving operational efficiency, reducing costs and achieving strategic objectives. However, Outsourcing arrangements, if not effectively managed, can increase risk to the financial institution and threaten its safety and soundness. Therefore, Bank Negara Malaysia issued [Outsourcing](#) in 2019, clarifying the requirements and expectations for financial institutions to maintain appropriate internal governance and outsourcing risk frameworks. The requirements also serve to ensure the Bank's continued ability to carry out effective supervisory oversight over financial institutions in relation to their outsourced activities. Its provisions primarily focus on outsourcing process and management of risks, outsourcing outside Malaysia, and outsourcing involving cloud services.

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

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.2-9.3	Assessment of service provider	9.2 Conducting a comprehensive and robust due diligence process is necessary for a financial institution to make an informed selection of service providers in relation to the risks associated with the outsourcing arrangement.	When considering new outsourcing, renewal of existing arrangements, or renegotiation of current agreements, customers should conduct a comprehensive due diligence on the service provider, covering various aspects such as capabilities, qualifications, financial strength, business reputation, information security, operational location, data protection, and subcontractor management.
		9.3 A financial institution must conduct appropriate due diligence of a service provider at the point of considering all new arrangements and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process must be commensurate with the materiality of the outsourced activity.	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:
		The due diligence process must cover, at a minimum—	(a) capacity, capability, financial strength and business reputation
		(a) capacity, capability, financial strength and business reputation; (b) risk management and	• 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		internal control capabilities, including physical and IT security controls, and business continuity management; (c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites; (d) access rights of the financial institution and the Bank to the service provider; (e) measures and processes to ensure data protection and confidentiality; (f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement; (g) undue risks resulting from similar business arrangements, if any, between the service provider and the financial institution; (h) the extent of concentration risk to which the financial institution is exposed with respect to a single service provider and the mitigation measures to address this concentration. This does not apply to a service provider that is an affiliate and is supervised by a financial regulatory authority; and (i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy	numerous enterprises and government agencies. Financial Strength: Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant. Technical strengths: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products, ensuring reliable and continuous service for customers. Capability: Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. Specifically for Malaysia, Tencent Cloud has completed IT compliance audits tailored to Malaysia's financial industry conducted by independent third parties, which demonstrates that Tencent Cloud's security management and privacy protection frameworks meet the relevant certification

No.	Domain	Summary of Controls	Tencent Cloud's Response
		document.	standards and industry best practices.
			(b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management Physical Security: Tencent Cloud has established a physical security management framework to regulate operational safety, promptly identify risks, and enhance physical security controls. All Tencent Cloud data centers worldwide are selected, constructed, or leased in accordance with international standards and local security requirements. Data centers are equipped with fully redundant power and cooling systems to prevent single points of failure. Fire protection systems include localized fire detection, automatic suppression systems, and manual firefighting equipment. Anti-static flooring and grounded racks and cable trays are installed to protect equipment from electrostatic damage. Information Security: Tencent Cloud has built an information security management system based on industry standards and best practices to support secure cloud operations. The security policy framework includes strategic direction, organizational structure, and management systems. Policies are reviewed annually to ensure alignment with security objectives, standards, procedures, and legal requirements. Employees can access these policies via Tencent Cloud's internal platform. Business Continuity: Tencent Cloud is certified under ISO/IEC 22301 for Business Continuity Management. Business impact analyses are conducted for cloud products and services, and corresponding continuity and disaster

No.	Domain	Summary of Controls	Tencent Cloud's Response
			recovery plans are developed. Detailed recovery plans are in place for critical products and processes, with regular drills conducted to ensure timeliness and effectiveness. (c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites Tencent Cloud's infrastructure spans multiple global locations, organized by regions and availability zones. Each region is an independent geographic area, and each availability zone is an independent fault isolation domain with physical separation. Customers can flexibly deploy data and systems across different regions or zones based on business needs and data security requirements to meet disaster recovery objectives. In 2026, Tencent Cloud launched three data centers in Malaysia, offering a range of cloud computing services including cloud servers, cloud databases, and CDN. Customers can independently choose the location for storing and processing their data based on their business location and preferences. (d) access rights of the financial institution and the Bank to the service provider Tencent Cloud will provide dedicated assistance and actively cooperate with customers and the Bank in audits and supervisory reviews as required. (e) measures and processes to ensure data protection and confidentiality 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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			of Customer data, intellectual property, and 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. (f) reliance on sub-contractors, if any, where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement Tencent Cloud publishes the online Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, and other legal documents on its international portal. For sub-processing scenarios, these agreements expressly set out clauses on prior consent to sub-processing, advance notice of any addition or replacement of sub-processors, and data-protection obligations. Tencent Cloud will not sub-contract any processing activities performed on behalf of the customer under the relevant contract/agreement without the customer's prior written consent. Any anticipated change involving the addition or replacement of a sub-processor will be notified to the customer by e-mail or other agreed channels. Customers may also elect to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. . For subcontractor management, Tencent Cloud maintains a comprehensive supply-chain security management system. Through rigorous supplier security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements, Tencent Cloud exercises effective control over its suppliers to ensure that sub-processing does not impair its ability to provide the relevant services to customers, the confidentiality and integrity of customer information handling, or the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. (h) the extent of concentration risk to which the financial institution is exposed with respect to a single service provider and the mitigation measures to address this concentration 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 supports customers in building hybrid cloud and multi-cloud architectures by providing standardized APIs and data migration tools to reduce the risk of vendor lock-in. (i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document The Tencent Cloud security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual professional audits by independent third parties both

No.	Domain	Summary of Controls	Tencent Cloud's Response
			domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center .
9.6	Outsourcing agreement	9.6 An outsourcing arrangement must be governed by a written agreement that is legally enforceable. The outsourcing agreement must, at a minimum, provide for the following– (a) duration of the arrangement with date of commencement and expiry or renewal date (b) responsibilities of the service provider (c) controls to ensure the security of any information (d) use of information shared with the service provider is limited to the extent necessary to perform the obligations under the outsourcing agreement (e) continuous and complete access by the financial institution to its data held by the service provider in the event of a dispute with the	Customers should enter into an outsourcing agreement with the service provider that covers the scope of the arrangement, performance and risk management standards, confidentiality and security obligations, business continuity, monitoring and control mechanisms, audit rights, notification of adverse events, dispute resolution, termination and early exit provisions, and applicable laws. The agreement must ensure legal validity and enforceability. Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly set out the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, the service term and termination scenarios, the dispute-resolution mechanism, and the notice procedure. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		service provider, or termination of the arrangement (f) ability of the financial institution and its external auditor to conduct audits and on-site inspections on the service provider and its subcontractors, and to obtain any report or finding made in relation to the outsourced activity (g) notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations (h) measures that the service provider would take to ensure continuity of the outsourced activity in the event of an operational disruption or failure on the part of the service provider (i) regular testing of the service provider's business continuity plans (BCP), including specific testing that may be required to support the financial institution's own BCP testing, and a summary of the test results to be provided to the financial institution with respect to the outsourced activity (j) the dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant	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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(k) circumstances that may lead to termination of the arrangement, the contractual parties' termination rights and a minimum period to execute the termination provisions, including providing sufficient time for an orderly transfer of the outsourced activity to the financial institution or another party (l) where relevant, terms governing the ability of the primary service provider to sub-contract to other parties (m) corresponding obligations for staff of the service provider, who are involved in the delivery of services to the financial institution's customers, to comply with similar conduct standards imposed by the Bank on the financial institution.	
9.7, 9.8	Protection of data confidentiality	9.8 Misuse, unauthorised or inadvertent disclosure of confidential information is a serious risk event for financial institutions. It is therefore imperative that the financial institution satisfies itself that the level of security controls, governance, policies, and procedures at the service provider are robust to protect the security and confidentiality of information shared under the outsourcing arrangement. 9.9 A financial institution must ensure that appropriate controls are in place and are effective in	Customers should ensure that the service provider implements the necessary security governance, controls, policies and procedures to safeguard the security, confidentiality and integrity of the information. To assist customers in meeting regulatory requirements, in terms of data usage and access, customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents). Tencent Cloud enforces end-to-end identity

No.	Domain	Summary of Controls	Tencent Cloud's Response
		safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, the financial institution must ensure that— (a) information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and only on a need-to-know basis; (b) information shared with the service provider is used only to the extent necessary to perform the obligations under the outsourcing agreement; (c) all locations (e.g. city and country) where information is processed or stored, including back-up locations, are made known to the financial institution; (d) where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia; (e) where the service provider provides services to multiple clients, the financial institution's information must be segregated from the information of other clients of the service provider; (f) the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even	verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities. Tencent Cloud's internal office network is completely isolated from the production environment where customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-factor authentication. Tencent Cloud adopts fine-grained permission division during permission granting, only granting employees the minimum operational permissions and time limits necessary to provide services. All backend operational records are centrally stored by the log platform and are regularly reviewed by Tencent Cloud's internal audit team. Regarding the locations where all the customer information is processed or stored, Tencent Cloud's infrastructure spans multiple global locations, organized by regions and availability zones. Each region is an independent geographic area, and each availability zone is an independent fault isolation domain with physical separation. Customers can flexibly deploy data and systems across different regions or zones based on business needs and data security requirements to meet disaster recovery objectives. In 2026, Tencent Cloud launched three data centers in Malaysia, offering a range of cloud computing services including cloud servers, cloud databases, and CDN. Customers can independently choose the location for storing and processing their data based on their business location and preferences. Tencent Cloud adheres to principles of transparency. Upon request, Tencent Cloud will

No.	Domain	Summary of Controls	Tencent Cloud's Response
		after the arrangement has ceased; and (g) information shared with the service provider is destroyed, rendered unusable, or returned to the financial institution in a timely and secure manner once the outsourcing arrangement ceases or is terminated.	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. For tenant isolation, Tencent Cloud enforces resource access control at the virtualization layer, private network isolation policies, web console permission management, identity verification, and secure API session handling. These mechanisms ensure that each customer can only access their purchased resources, effectively preventing cross-tenant data access or tampering. If customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate cloud data and production environments at any time. According to the service agreement between Tencent Cloud and the customer, if the cloud service expires or is terminated, customers must complete data migration before the retention period ends for any data stored on cloud servers through Tencent Cloud services. Tencent Cloud supports customers in backing up and migrating data using common standard formats. Customers can use the same transmission methods and protocols as during onboarding or leverage network services such as Direct Connect (DC) and VPN Connection to ensure secure and reliable data transfer during offboarding. After cloud services are terminated, Tencent Cloud will follow strict data erasure procedures and permanently delete all customer data, including replicas and backups, after the retention period. Deleted data cannot be restored.
9.10 、 9.12- 9.14	Business continuity planning	9.10 A financial institution is responsible for ensuring that its BCP consider any operational disruptions at, or failure of, the service provider.	Customers should ensure that their business continuity plan fully considers the risks of operational disruptions or failures of the service provider. In the event of an interruption material outsourced activities must be restored without causing significant business impacts.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		9.12 In the event of a disruption, material outsourced activities must be resumed without undue delay and with minimal impact and disruptions to both business operations and the financial institution's customers.	Additionally, customers should be able to access all the records and information stored at the service provider at any time. Customers should also regularly test their business continuity plan and require their service provider to conduct business continuity tests on a regular basis. In case of necessity, joint tests should also be carried out.
		9.13 A financial institution must, at all times, ensure that it has ready access to all its records and information at the service provider with respect to the outsourced activity which would be necessary for it to operate and meet its legal and regulatory obligations. This includes scenarios where network connectivity is not available, the service provider becomes insolvent or a dispute resolution process is ongoing.	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.
		9.14 A financial institution must periodically test its own BCP and proactively seek assurance on the state of BCP preparedness of the service provider and where relevant, alternative service providers. The intensity and regularity of the BCP testing and assessments of BCP preparedness must be commensurate with the materiality of the outsourcing arrangement. In assessing this preparedness, the financial institution must, at a minimum— (a) ensure that the back-up arrangements are available and ready to be operated when	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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		necessary; (b) ensure that the service provider periodically tests its BCP and provides any test reports, including any identified deficiencies, that may affect the provision of the outsourced service and measures to address such deficiencies as soon as practicable; and (c) for material outsourcing arrangements, participate in joint testing with the service provider to enable an end-to-end BCP test for these arrangements by the financial institution.	Section 8: “How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Business Continuity Management”.
10.1-10.3	Outsourcing outside Malaysia	10.1 Outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia exposes a financial institution to additional risks (e.g. country risk). A financial institution should have in place appropriate controls and safeguards to manage these additional risks, having regard to social and political conditions, government policies, and legal and regulatory developments. 10.2 In conducting the due diligence process, a financial institution must ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the financial	When customers engage a service provider from outside Malaysia, they should continuously consider factors such as government policies, political and social environments, foreign laws and regulations, as well as business continuity management on the basis of due diligence. Customers should also ensure Bank's ability to exercise its regulatory or supervisory powers. Tencent Cloud builds or leases data centers in multiple global locations in accordance with relevant international standards and local security requirements. Tencent Cloud offers multi-region and multi-availability zone options and strictly complies with applicable laws and regulations in each jurisdiction to protect user privacy and data security, while actively monitoring local regulatory developments. Customers may flexibly deploy data and systems across different regions or availability zones based on business needs and data security requirements. To ensure continuous availability of Customer operations, Tencent Cloud's compute, network, storage, database, container, middleware, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		institution or service provider to implement appropriate responses to emerging risk events in a timely manner. 10.3 A financial institution must ensure that outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect— (a) the financial institution's ability to effectively monitor the service provider and execute the institution's BCP; (b) the financial institution's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and (c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity.	security services are designed for high availability and supported by disaster recovery plans. Tencent Cloud has established a comprehensive internal business continuity management system and is certified under the ISO/IEC 22301 international standard for business continuity management. Upon customers request, Tencent Cloud will actively cooperate by providing information and, where necessary, furnish Bank or its designated personnel with records, documents, reports, or information related to the confidentiality and integrity of customer information.
11.1-11.4	Response and recovery	11.1 Where the outsourcing arrangement involves a cloud service provider, a financial institution should take effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance. This is particularly important as cloud service providers often operate a geographically dispersed	Where the outsourcing arrangement involves a cloud service provider, customers should take into account compliance risks such as data accessibility, confidentiality, sovereignty, and recoverability. Customers should also agree with the cloud service provider and its subcontractors to retain the rights for auditing and inspection, or obtain third-party certifications and reports. At the same time, customers can request the cloud service provider to provide a business continuity test report. In terms of data accessibility, Cloud Access

No.	Domain	Summary of Controls	Tencent Cloud's Response
		computing infrastructure with regional or global distribution of data processing and storage.	Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources.
		11.2 In using cloud services, the inherent risks involved are similar to that of other forms of outsourcing arrangements. A financial institution that subscribes to cloud services must comply with the requirements of this policy document, and other relevant requirements on cloud services as specified by the Bank.	For data storage protection, Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption keys are managed through the integrated Key Management Service (KMS), which provides full lifecycle management. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • Cloud Connect Network (CCN): CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal path selection, and fast failover capabilities.
		11.3 In relation to a financial institution's ability to conduct audits and inspections on the cloud service provider and sub-contractors pursuant to paragraph 9.6(f), the financial institution may rely on third party certification and reports made available by the cloud service provider for the audit, provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit.	
		11.4 In relation to the testing of a cloud service provider's BCP pursuant to paragraph 9.6(i), a financial institution must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising	In terms of the ownership of customer data,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		from the BCP testing.	customer data is classified as a high-security-level data within Tencent Cloud. Customers retain exclusive ownership and control over their data content. On its international portal, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, the service term, and the scenarios under which the agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. From a compliance perspective, Tencent Cloud strictly adheres to laws and regulations governing user privacy and data security in the jurisdictions where it operates. Tencent Cloud has obtained several security and privacy compliance certifications and qualifications, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC, and undergoes annual audits by professional third-party audit institutions. Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. These certifications demonstrate that Tencent Cloud's security management and personal data protection practices meet relevant certification standards or industry's best practices. For more detailed information about the authoritative certifications obtained by Tencent Cloud and the completed third-party independent evaluations/audits, please refer to Section 2 "Tencent Cloud Security and Privacy Compliance". For business continuity testing, Tencent Cloud develops tailored disaster recovery strategies and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. For more details on business continuity, refer to Section 8: “How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Business Continuity Management”.

06

How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Management of Customer Information and Permitted Disclosures

Financial service providers (FSPs)¹ handle a significant amount of customer information while providing financial services and products. Proper handling of customer information is crucial for building public trust and confidence, and for maintaining the brand and good reputation of financial service providers. Therefore, BNM has issued the [Management of Customer Information and Permitted Disclosures](#), requiring FSPs to protect customer information against theft, loss, misuse or unauthorised access, modification or disclosure by whatever means, including disclosure made in verbal or written form. This Policy Document sets out Bank Negara Malaysia's requirements and expectations with regard to FSPs' measures and controls in handling customer information, throughout the information lifecycle, covering collection, storage, use, transmission, sharing, disclosure and disposal of customer information. The requirements mainly focus on areas such as risk assessment, policies and procedures, information and communication technology (ICT) controls, access controls, physical security, staff, Representatives, Agents and External Vendors' Personnel, customer information breaches and Outsourced service provider.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in Management of Customer Information and Permitted Disclosures, and explains how Tencent Cloud, as a cloud service provider, assists financial service providers in complying with these requirements.

6.1 Control environment

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.1-10.3	Risk assessment	10.1 FSPs must identify and address potential threats and vulnerabilities that could result in theft, loss, misuse, or unauthorised access, modification or disclosure by whatever means, of customer information.	Customers should identify potential threats and vulnerabilities, and assess the likelihood of their occurrence, as well as the potential impact they may have if a security incident occurs. 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
		10.2 FSPs must also assess the likelihood that identified threats and vulnerabilities will materialise, and the potential impact on both the FSP and its customers in the event a customer information breach occurs. This assessment, among other considerations,	

¹ Financial service providers (FSPs): including: (a) a licensed bank; (b) a licensed investment bank; (c) a licensed Islamic bank; (d) a licensed international Islamic bank; (e) a licensed insurer; (f) a licensed takaful operator; (g) a licensed international takaful operator; (h) a prescribed institution; (i) an approved insurance broker; (j) an approved takaful broker; (k) an approved financial adviser; (l) an approved Islamic financial adviser; (m) an approved money broker; (n) an approved issuer of a designated payment instrument; (o) an approved issuer of a designated Islamic payment instrument; (p) an approved operator of a payment system; (q) a registered operator of a payment system; and (r) a registered adjuster.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		must include third-party service providers and outsourcing arrangements, and be supported by mitigation plans that are developed and implemented based on the threats identified.	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, 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. In addition, Tencent Cloud has defined an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessments regularly, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. At the same time, Tencent Cloud has established an internal vulnerability scanning mechanism and an external vulnerability collection platform. Tencent Cloud uses a vulnerability scanning system to perform regular scans for security vulnerabilities across the cloud environment. The scanning scope covers the virtualization layer, system layer, and
	10.3	Threats and vulnerabilities to customer information can be internal or external and could be due to negligence or a deliberate act of any person.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			application layer. Upon completion of the scanning, the Tencent Cloud security team will analyze, categorize, and address the discovered vulnerabilities. Any identified security vulnerabilities are logged into the ticketing system to ensure they are properly handled within the stipulated timeframe.
10.6 、 10.9- 10.11	Policies and procedures	10.6 FSPs must establish and have in place written policies and procedures to safeguard customer information, and this must include the collection, access, storage, use, transmission, sharing, disclosure and disposal of customer information. 10.9 FSPs may incorporate the requirements on the proper handling of customer information in other policies, if appropriate. These may include written policies on human resource, code of conduct, information security, outsourcing and the disclosure of customer information to parties permitted under the law. 10.10 FSPs must ensure that the written policies and procedures are readily accessible and clearly communicated to staff by the person designated under paragraph 9.2, to ensure compliance with such policies and procedures. 10.11 FSPs must continually review their written policies and procedures to ensure that they remain adequate, relevant	Customers should formulate policies and procedures for protecting customer information, manage the collection, access, storage, use, transmission, sharing, disclosure and disposal of customer information, and incorporate these requirements into policies such as human resources, information security, and code of conduct. Customers should also regularly communicate these requirements to employees. Customers should also continuously review the relevant written policies and procedures and update them as needed. To implement personal information protection and management, Tencent Cloud has established personal information management policies and procedures. These are designed to process personal information generated by customers during registration, purchase, and use of cloud services in accordance with the principles of legality, legitimacy, and minimal necessity. They also empower customers to manage their data and fulfill privacy protection obligations through various tools and services. The relevant policies and procedures specify requirements for the collection, use, storage, disclosure, restriction of processing and deletion of personal information, the concept of privacy by design, the handling of customer personal information after service termination, and the exercise of customer rights. Tencent Cloud annually reviews these policies and requirements to ensure that control objectives, control procedures, and control measures align with relevant security strategies, standards, procedures, and legal requirements, thereby

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and operate effectively in response to changes in the operating environment.	guaranteeing the adequacy and effectiveness of the policies.
10.12, 10.13	Information and communication technology (ICT) controls- preventive and detective ICT controls	10.12 FSPs must deploy preventive and detective ICT controls to- (a) prevent theft, loss, misuse or unauthorised access, modification or disclosure of customer information; and (b) detect errors and irregularities when they occur. 10.13 FSPs must regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats.	Customers should implement preventive and detective ICT controls to prevent their information from being accessed, modified or disclosed without authorization, and to promptly detect errors and irregularities. Additionally, customers should monitor the effectiveness of these controls. Tencent Cloud offers a variety of cloud products/services to assist customers in implementing preventive control measures, such as: • <u>Cloud Access Management (CAM)</u> helps customers securely and granularly manage access to Tencent Cloud products and resources. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. • Customers can use <u>Cloud Workload Protection Platform (CWPP)</u>, which leverages Tencent's extensive threat intelligence to help manage baseline security. CWPP supports baseline detection through options such as one-click checks and scheduled scans, and provides visibility into baseline compliance rates along with remediation recommendations. CWPP also offers Tencent Cloud's default baseline policies to help customers better manage server security baselines. • <u>Cloud Security Center (CSC)</u> provides automated configuration risk assessment for cloud products, covering cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			servers, object storage, cloud databases, and load balancers, helping customers reduce risks caused by misconfigurations and improve overall cloud security posture. Customers can use Configuration Audit (Config) for centralized auditing and governance of cloud resources, continuously recording configuration details and changes across regions under the customer's account. Based on Tencent Cloud best-practice rules and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. To support regulatory compliance, Tencent Cloud has also established internal access control authorization policies and a role-separation matrix. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions only when necessary and through a rigorous approval process. Tencent Cloud has established a set of network security configuration standards and security baseline standards aimed at standardizing the security configuration of network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud uses scanning tools to check the configurations of operating systems, database management systems, network devices, and virtual images, continuously detecting deviations from the standard configurations defined in baseline files. Tencent Cloud offers a variety of cloud products/services to assist customers in implementing detective control measures,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			such as: - Customers may use Cloud Log Service (CLS), a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. - 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. Cloud Firewall (CFW) provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. Web Application Firewall (WAF) helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. To assist customers in complying with regulatory requirements, Tencent Cloud employs multiple protective mechanisms, including firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS protection, and web security protection, to counter various threats from the internet. Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.14、 10.15	Information and communication technology (ICT) controls-remote access	10.14 On occasions where FSPs' staff, representatives and agents undertake offsite work arrangements, FSPs must have in place appropriate controls for such offsite work arrangements including for the ICT equipment used that allow access into FSPs' systems and customer information.	prevent abnormal system activities and risks. Tencent Cloud also operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls. In addition, Tencent Cloud has defined detailed operational security "red lines" and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts. For employee's offsite work, customers should establish remote access control measures for the ICT devices used to access the financial services system and customer information, such as implementing strong identity authentication mechanisms, encrypting data stored on the ICT equipment, and protecting data transmission securely.
		10.15 The controls referred to in paragraph 10.14 may include robust authentication for remote access into FSPs' systems, encrypting data stored on the ICT equipment and ensuring data transmission is securely protected.	To enable customers to securely and quickly access cloud business systems anytime, anywhere, and from any mainstream device, Tencent Cloud supports SSL VPN technology for remote access. SSL VPN encrypts data transmitted over the Internet to ensure security and provides access control mechanisms to reduce unauthorized access. In terms of remote access, Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect through encrypted communication channels to access Tencent Cloud's corporate network and office systems remotely. Furthermore, Tencent Cloud's internal office network is completely isolated from the production environment where Customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-

No.	Domain	Summary of Controls	Tencent Cloud's Response
			factor authentication. Tencent Cloud maintains remote access logs to record user activities. All backend maintenance operations are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these records. To protect stored data, Tencent Cloud's storage and database products support encryption using strong algorithms and integrate with Key Management Service (KMS) for full lifecycle key management. 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.
10.16、10.17	Information and communication technology (ICT) controls-storage devices	10.16 FSPs must ensure that only staff with a legitimate business need is allowed to download customer information into portable storage devices provided by the FSP. 10.17 FSPs must put in place	Customers should ensure that only employees with legitimate business needs is allowed to download customer information into portable storage devices provided by their company and implement adequate protection measures for the information on the devices, such as passwords and data encryption. Customer data is classified as high-security data

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the relevant controls to ensure that the customer information stored in such portable storage devices pursuant to paragraph 10.16 is adequately protected, such as password and data encryption, to prevent theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.	within Tencent Cloud. Unless it is necessary to provide services or resolve technical issues, and only with explicit customer authorization or in accordance with investigations by national or local government departments into criminal activities that comply with national laws and regulations, Tencent Cloud employees will never proactively access any customer data. Tencent Cloud's production environment is securely isolated from the office environment. By default, exporting, copying, or downloading customer data from the production environment is prohibited. To assist customers in complying with regulatory requirements, Tencent Cloud has established relevant standards for mobile office security management regarding the use of mobile devices and bring-your-own-device (BYOD) management, specifying security requirements for internal mobile device usage. Employees must strictly adhere to the company's endpoint control and access requirements when using mobile devices. For data identified as sensitive on devices, Tencent Cloud employs encryption and data leakage prevention technologies to prevent illegal or accidental data leakage. Tencent Cloud has deployed a zero-trust security management system to conduct security controls. Leveraging the system's security capabilities including virus scanning and removal, vulnerability remediation, and active defense, it achieves comprehensive security protection against ransomware, phishing attacks, and internal lateral movement. The zero-trust security management system also supports the sensitive data exfiltration monitoring function, which can audit and block file exfiltration activities via email, cloud storage services, remote control tools, file transfer tools, and other channels, preventing potential data theft incidents.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			At the same time, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. The EDR tools support antivirus and intrusion detection, security baseline and vulnerability scanning, and compliance auditing of command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviours.
10.20-10.21	Information and communication technology (ICT) controls- unauthorised disclosure	10.20 FSPs must have in place mechanisms that create a strong deterrent effect against unauthorised disclosure by whatever means of customer information by staff. 10.21 Unauthorised disclosure may occur in many ways and forms such as staff taking photograph of documents or screens that contain customer information. The mechanisms referred to in paragraph 10.20 may include raising staff awareness on the disciplinary actions for unauthorised disclosure by whatever means, installing CCTV at relevant areas, having an open office concept, encouraging whistleblowing in this respect, or restricting personal electronic devices at high risk areas like data centres, dealing rooms, call centres, etc.	Customers should implement necessary security measures to prevent unauthorised disclosure by whatever means of customer information by staff, such as establishing employee reward and punishment mechanism, installing surveillance devices, and restricting the use of personal electronic devices, etc. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed. To strengthen employees' awareness of information security and data protection, and to prevent the risks of illegal data theft or accidental leakage, Tencent Cloud promotes various security behavioral standards to employees through activities such as security awareness training, production of security promotion posters, and educational videos. These initiatives continuously enhance the entire staff's capabilities in data security protection and compliance awareness. In terms of mobile device usage and bring-your-own-device (BYOD) management, Tencent Cloud has established relevant standards for mobile office security management, specifying security requirements

No.	Domain	Summary of Controls	Tencent Cloud's Response
			for the use of internal mobile devices. Employees must strictly adhere to the company's endpoint control and access requirements when using mobile devices. In terms of physical security in the office area, physical access to Tencent Cloud office areas is controlled through multiple security measures, including security personnel, access card systems, and CCTV monitoring. Visitors are only permitted with prior approval from Tencent Cloud staff. Visitors must register with security and deposit electronic devices before entering. The carrying of any portable storage devices into the data center is strictly prohibited. All visitors must be accompanied by authorized personnel at all times while in controlled areas of the data center. All activities within office areas are monitored via 24/7 CCTV surveillance. Tencent Cloud requires its employees to properly store paper documents containing sensitive information. After using public areas such as meeting rooms and training classrooms, employees must promptly erase confidential and sensitive information from whiteboards, turn off projectors, and retrieve meeting materials to prevent the leakage of confidential and sensitive information. A screen lock policy is implemented on Tencent Cloud employees' terminal devices to ensure the devices are locked when left unattended. Unattended equipment including copiers, fax machines, shredders, and printers is placed in monitored and appropriate locations within office areas to prevent unauthorized use and intrusion.
10.22	Information and communication technology (ICT) controls- internet browsing	10.22 FSPs must restrict access to web-based communication websites and social media platforms, particularly those which are encrypted from end-to-end (e.g., WhatsApp Desktop,	Customers should impose restrictions on the access of employees handling customer information to web-based communication websites and social media platforms. Tencent Cloud has established network security management standards and a

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Facebook and Skype Messenger) on staff who handle customer information, to prevent unauthorised disclosure of customer information to external parties via internet services.	defense-in-depth architecture. Security domains are defined based on business functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time. In terms of internet browsing security, Tencent Cloud's network team has implemented multiple protective measures. These include unified control of internet browsing channels, enabling web security filtering and malicious URL blocking, deploying endpoint security and antivirus software, and providing employees with security awareness training on safe internet browsing. These measures ensure the security of connections between internal networks and the internet.
10.23 、 10.24	Information and communication technology (ICT) controls-access controls	10.23 FSPs must also implement mechanisms for the prompt detection of- (a) unauthorised access to customer information; (b) unusual frequent viewing of customer information in the FSPs' systems by staff; (c) unusual or suspicious downloading activities that involve customer information; and (d) unauthorised disclosure of customer information to external parties. 10.24 The mechanisms referred to in paragraph 10.23 may include installing key-logger software, conducting regular reviews of audit trail and carrying out random periodic sample checks.	Customers should establish an access control management mechanism to promptly detect any unauthorized or suspicious behavior regarding customer information. Access authorization should be based on the storage location of customer information in different systems. The access rights should be clearly stated in the job descriptions of employees. Regular reviews of employee access rights should be conducted, and unnecessary permissions should be promptly removed. <u>Cloud Access Management (CAM)</u> helps customers securely and granularly manage access to Tencent Cloud products and resources. CAM also supports multiple secondary authentication methods, and supports viewing and tracking employee operation records through <u>CloudAudit</u>. In addition, Tencent Cloud provides <u>Bastion Host (BH)</u>, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.25-10.27	Access controls	10.25 FSPs must ensure that the role profile for each type of job includes a description of the access rights to customer information if relevant, for staff to perform their jobs in accordance with the access rights. 10.26 FSPs must identify the location of customer information residing in different systems and ensure that adequate access controls are in place at different levels (i.e. application level, database level, operating system level and network level) to prevent unauthorised access, modification or disclosure by whatever means of customer information to external parties. 10.27 FSPs must regularly review the access rights of staff and immediately revoke the access rights of any staff leaving the FSP or changing to a new role or position that does not require access to customer information to prevent the theft of customer information.	access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Tencent Cloud has also established internal access control authorization policies and has standardized the access control activities for cloud platform products, terminal systems, host operating systems, application systems, and network devices. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud enforces zero-trust security management for employee access, requiring login and completion of multi-factor authentication before accessing internal resources. 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 mapping job roles to identity information and system permission levels and conducts regular internal permission reviews to prevent misuse or abuse of access rights. Tencent Cloud implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the IT security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.28-10.31	Physical security	10.28 FSPs must implement adequate physical security controls to ensure customer information stored either in paper or electronic forms are properly protected against theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.	Customers should implement physical environment security control measures to protect customer information in both paper and electronic forms from security risks. Customers should properly handle customer information collected off-site and in-transit and implement strong preventive measures for physical areas where large amounts or critical sensitive customer information is stored. Customers should also implement a desktop cleaning policy.
		10.29 FSPs must restrict access and implement robust intruder deterrents in areas where large amounts, or critical and sensitive customer information, are accessible and stored, for example, the server and filing rooms.	In terms of physical security in the office area , physical access to Tencent Cloud office areas is controlled through multiple security measures, including security personnel, access card systems, and CCTV monitoring. Visitors must register with security and deposit electronic devices before entering. The carrying of any portable storage devices into the data center is strictly prohibited. All visitors must be accompanied by authorized personnel at all times while in controlled areas of the data center. All activities within office areas are monitored via 24/7 CCTV surveillance.
		10.30 To minimise the risks of theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information, FSPs may consider implementing a clear-desk policy.	Tencent Cloud requires its employees to properly store paper documents containing sensitive information. After using public areas such as meeting rooms and training classrooms, employees must promptly erase confidential and sensitive information from whiteboards, turn off projectors, and retrieve meeting materials to prevent the leakage of confidential and sensitive information. A screen lock policy is implemented on Tencent Cloud employees' terminal devices to ensure the devices are locked when left unattended. Unattended equipment including copiers, fax machines, shredders, and printers is placed in monitored and appropriate locations within office areas to prevent unauthorized use and intrusion.
		10.31 FSPs must provide clear policy and procedures encompassing adequate controls to be put in place for the proper handling of customer information collected off-site and in-transit. This must include ensuring that physical documents are securely stored while the customer information stored in portable devices are securely protected to prevent theft, loss, misuse or unauthorised access, modification or disclosure by	In addition, Tencent Cloud requires data center operators to establish a comprehensive

No.	Domain	Summary of Controls	Tencent Cloud's Response
		whatever means.	personnel access control security matrix within the access authorization system based on personnel categories and access privileges, so as to achieve effective management and control over the access, operations, and other behaviors of various personnel. Tencent Cloud mandates operators to verify the identity of all visitors or staff entering and exiting the data center, inspect their personal belongings, and register the items they carry. For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration.
10.32-10.37	Physical security - information destroy	10.32 To effectively safeguard customer information throughout its lifecycle, FSPs must have proper procedures in place to identify customer information that is no longer required from the perspective of the operation or requirements of any written law. FSPs shall deploy appropriate methods to securely dispose of such customer information which includes any paper and digital records of the customer information. 10.33 Customer information is considered securely disposed	Customers should dispose of the no-longer-needed customer information in an appropriate manner to ensure that it cannot be recovered. For the destruction of electronic devices, proper sanitization using industry standard method should be adopted. If the destruction is entrusted to an outsourcing service provider for transportation to an off-site location, risks and benefits need to be evaluated, and random inspections of the destruction process carried out by the outsourcing service provider should be conducted on a regular basis. Tencent Cloud stores and disposes of media based on the sensitivity level of the information contained therein and has established media management procedures that specify the specific processes and standards for media storage and disposal. Prior to media disposal,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		of when it is beyond any possibility of recovery, is irreversible or cannot be reconstructed in any way. 10.34 To ensure secure data destruction, all devices may undergo proper sanitization using industry standard method and chain of custody controls, such as data wiping software, physical destruction or degaussing. For information stored in digital devices, a simple file deletion or reformatting of hard drives and portable storage devices may not be sufficient to completely destroy the stored information. 10.35 FSPs must assess the risks and benefits of engaging an outsourced service provider for the destruction of customer information which involves transporting customer information outside the FSP's premises. 10.36 FSPs must shred or store customer information in a manner that is inaccessible such as sealed in bags with tamper proof fasteners or stored in locked containers before it is collected by outsourced service providers for destruction. 10.37 FSPs must conduct random checks on the collection and destruction process carried out by outsourced service providers	relevant approvals must be obtained, and detailed records of the disposal process shall be kept. Depending on the material, storage principle, and the sensitivity level of the information stored, the designated team will adopt targeted disposal methods to ensure that the data is irrecoverable, and the disposal complies with security specifications. Tencent Cloud tracks the entire process of media outbound, transportation, and inbound through a work orders. During transportation, Tencent Cloud selects secure and reliable carriers, implements protective measures in accordance with the information classification level, and applies protective packaging to physical media to prevent physical damage during transit. Tencent Cloud provides a secure and reliable data destruction mechanism. Upon termination of a customer's service, Tencent Cloud follows strict data erasure methods to completely delete customer data before reusing the previously purchased computing and storage resources. If media used to deliver Tencent Cloud services fails and requires replacement or reaches end-of-life, Tencent Cloud promptly performs thorough physical destruction in accordance with strict processes.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		to ensure that customer information is properly destroyed.	
10.39-10.46、10.49	Staff, Representatives, Agents and External Vendors' Personnel	10.39 FSPs must ensure that employment contracts contain a provision requiring all staff to sign a confidentiality undertaking that clearly specifies the obligation and requirement under the relevant written law to safeguard customer information as well as the consequences for failure to comply with such obligation and requirement. 10.40 Where FSPs engage with external vendors to carry out duties or services within the FSPs' premises (e.g., security guards, cleaners and maintenance officers/engineers), FSPs must ensure that the external vendors carry out an appropriate level of vetting and monitoring on their personnel to reduce the risk of customer information theft. 10.41 FSPs must ensure a high degree of staff awareness at all times on the following: (a) the need to protect the confidentiality and security of customer information; (b) the importance of complying with relevant policies and procedures established by the FSPs; and (c) the consequences if any	Customers should ensure that all employees understand the significance of protecting the confidentiality and security of customer information. Customers should conduct training to enhance employees' awareness, establish a reward and punishment mechanism, regularly assess and investigate the effectiveness of the employee awareness training as well as the employees' compliance with relevant policies and procedures, and should sign a confidentiality commitment letter in the employment contract with the employees. To assist customers in complying with regulatory requirements, Tencent Cloud has established comprehensive human resource (HR) management standards and procedures to ensure the selection, recruitment, and assignment of personnel in line with job requirements. Tencent Cloud has defined a clear employee lifecycle framework, covering pre-employment procedures, on-the-job procedures, and offboarding procedures. Prior to onboarding, applicants undergo interviews, during which Tencent Cloud assesses their competence to meet the job requirements. In accordance with applicable laws and job levels, the HR department conducts pre-employment background checks on candidates. These checks include verification of past work experience, criminal background screening, and educational qualification verification. The results of background checks are documented in Tencent Cloud's HR management system. Upon accepting employment, internal employees are required to sign an employment

No.	Domain	Summary of Controls	Tencent Cloud's Response
		staff is involved in any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. 10.42 FSPs must have in place robust monitoring mechanisms to ensure that the relevant policies, procedures and controls established by the FSPs are adhered to by staff. 10.43 FSPs must provide relevant training and regularly remind all staff on their obligations to ensure the confidentiality of customer information is safeguarded when dealing with such information. 10.44 FSPs must include in their programme for new staff, specific trainings to explain the relevant policies and procedures on protecting customer information. 10.45 FSPs must ensure that new staff are notified on the possible actions that may be taken for non-compliance with policies and procedures. 10.46 Guidance provided to staff on safeguarding customer information should be concise and reader-friendly to enable understanding among staff on how to comply with the relevant policies and procedures. 10.49 FSPs must conduct a thorough and timely	agreement and an NDA. The employment agreement clarifies Tencent Cloud's existing security policies and the information security and personal data protection responsibilities to be fulfilled by employees or third parties. The NDA includes the signatory's confidentiality obligations and responsibilities, as well as potential penalties for violations of confidentiality clauses. Contract employees also undergo pre-employment background checks and are bound by the confidentiality requirements specified in the agreements signed between Tencent Cloud and the contracting agencies. The confidentiality requirements between Tencent Cloud and employees or third parties are reviewed and updated by the legal department as needed. During the employment tenure of employees or third-party personnel, the Human Resources Department conducts ongoing assessments of the security status of individuals with access to the cloud service management network or cloud service delivery network. Tencent Cloud has established a series of information security training and learning mechanisms to educate employees on information security policies, procedures, and guidelines. Employees are required to participate in regular information security awareness training. In terms of information security training and awareness dissemination, Tencent Cloud has implemented a comprehensive Information Security Training Framework, which requires all formal employees, consultants, interns, and outsourced staff to complete information security training courses. These courses include mandatory training for all staff, specialized training for key roles, and optional professional courses. The training content covers areas such as basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure

No.	Domain	Summary of Controls	Tencent Cloud's Response
		investigation 1 upon detecting theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information by staff and take appropriate actions against the staff concerned.	development practices, and data security requirements. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.
10.53- 10.56	Independent review	10.53 FSPs must subject their written policies, procedures and control measures for safeguarding customer information to an independent review at least once in every two years. 10.54 FSPs must ensure that the independent review must include an assessment of the effectiveness of senior management and their oversight as well as the adequacy and effectiveness of measures undertaken by the FSP to protect customer information from theft, loss, misuse or unauthorised access, modification or disclosure by whatever means. 10.55 The independent reviewer under paragraph 10.53 must communicate the written findings to the senior management and the Board of the FSP. 10.56 Based on the written findings under paragraph 10.55, senior management must ensure that appropriate	Customers are required to conduct an independent review of the written policies and procedures for customer information protection every two years, and submit the review results to the management. The management should take corrective measures promptly based on the review results. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments. Based on customer needs, Tencent Cloud also provides assurance reports on system and organizational controls to disclose the latest internal control status of its service organization to cloud customers, independent auditors, regulators, shareholders, and other stakeholders. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center. When selecting audit firms, Tencent Cloud follows the requirements outlined in this guide to ensure that the chosen firm has extensive project experience in Singapore's financial industry. Tencent Cloud also stipulates in its

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and timely actions are taken to rectify any deficiencies in the control measures.	agreements with audit firms that, in the event of a change of audit firm or auditor during the process, the outgoing auditor must properly hand over to the incoming auditor.

6.2 Customer information breaches

No.	Domain	Summary of Controls	Tencent Cloud's Response
11.1-11.5	Handling customer information breaches	11.1 FSPs must have in place a customer information breach handling and response plan to address any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. For the avoidance of doubt, FSPs must ensure that their customer information breach handling and response plans comprise of deliberate and non-deliberate customer information breaches. 11.2 The plan by FSPs under paragraph 11.1 must at a minimum, include escalation procedures and a clear line of responsibility to contain and take remedial actions relating to the customer information breach to prevent any future recurrence of the breach. 11.3 FSPs must ensure that all staff understand the escalation procedures and that the relevant staff are trained to effectively take the appropriate remedial actions for a customer information breach to protect affected	Customers should establish a mechanism for handling and responding to customer information breach, identify breach incidents and conduct investigations, and take mitigation measures to contain the breach of information. In the event of a large-scale breach, customers should assess the potential impact and report it to the BNM. For incident response and management, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. During the process of receiving, investigating, evaluating, handling and tracking information security incidents, the relevant responsible departments will maintain the relevant records of the received information security incidents and ensure the completeness and confidentiality of the records. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		customers' interests.	frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence.
		11.4 FSPs must have in place a mechanism to identify customer information breaches including those which arise from customer complaints and the FSPs must investigate the complaints promptly and properly.	In terms of communication and notification of the incident , Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses.
		11.5 FSPs must take appropriate mitigating actions to contain a customer information breach immediately.	To ensure the effectiveness and timeliness of the incident response process , Tencent Cloud conducts regular emergency drills related to security incident response and provides ongoing technical training to security team members. These training programs ensure that employees understand and comply with the latest security policies and procedures and are familiar with current information security standards and best practices.
			Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.
11.18-11.19、11.23	Submission of detailed investigation report	11.18 FSPs must carry out an investigation to ascertain the root causes of a customer information breach and determine appropriate remedial actions to prevent future recurrence. Additionally, FSPs must ensure that the investigation must be carried out by a competent party, overseen by a party independent of the relevant business unit where the breach occurred. 11.19 FSPs must complete the investigation within three (3) months upon detecting a customer information breach having regard to the complexity of the breach and table a detailed investigation report to the Board. 11.23 FSPs must put in place a register to record all customer information breaches covering the root causes, remedial actions and lessons learnt to prevent future recurrences.	Customers should investigate to determine the root cause of the customer information breach and take remedial measures to prevent future recurrence. Customers should also submit a detailed report to the management within three months after the incident occurs and submit the report to the BNM within one working day after submitting it to the management. To support customers in complying with regulatory requirements, in the event of a customer data breach, Tencent Cloud will record and track the security incident through its internal security operations system and notify affected customers in a timely manner as stipulated in the contract and required by regulations. The responsible departments will, upon completion of the incident remediation and handling, analyze the cause, type, losses, and responsibilities of the incident, compile an investigation and handling report on the information security incident, and collaborate with customers to complete the incident handling and reporting process. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type, frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management review.
11.25-11.31	Notification to affected customers	11.25 Where the customer information breach meets the definition of causing, or is likely to cause, significant harm as outlined in paragraph 11.10, the FSP must notify the affected customers without undue delay after the notification is made to BNM under paragraph 11.8. 11.26 With respect to paragraph 11.25, FSPs shall ensure any delay of the notification to the affected customers does not cause further harm to the affected customers. 11.27 When notifying affected customers under paragraph 11.25, FSPs must ensure that the affected customers, at a minimum, are provided with detailed information. 11.28 FSPs must ensure that notification to the affected customers is clear and written in plain language. The FSP must draw the customers' attention to the steps that they should take to protect themselves from any potential consequences in view of the customer information breach. 11.29 FSPs must notify the affected customers directly. However, in exceptional	If the breach of customer information meets the criteria for causing or potentially causing significant harm, customers should notify the affected customers in clear and concise language, including a brief description of the incident, its consequences, and the measures taken. Customers should also ensure that their employees have received training to handle inquiries from affected customers. 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,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		circumstances where direct notification would entail disproportionate effort, the FSP may issue a public announcement and display prominent notices at the FSP's branches and websites, provided such measures are sufficient. 11.30 In the event an FSP is unable to identify the specific customer(s) who are affected by a customer information breach at the point it is required to notify the affected customer under paragraph 11.25, the FSP must first notify its customers generally through a public announcement and display prominent notice at the FSP's branches and website. Upon identifying the specific affected customer(s), the FSP must notify the customer(s) directly, as soon as it is feasible to do so. 11.31 FSPs must ensure that their staff are trained to handle queries from the affected customers and to provide the necessary assistance on protective measures against any potential consequences that could be caused by the breach.	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.

6.3 Outsourced service provider

No.	Domain	Summary of Controls	Tencent Cloud's Response
12.2	Due diligence	12.2 FSPs must perform adequate and relevant due diligence assessments when selecting an OSP which has access to customer information including for processing, storing, or disposing customer information. These assessments will help FSPs understand the level of risks that may be introduced by the OSP and determine the appropriate monitoring that must be maintained.	Customers should perform adequate and relevant due diligence assessments when selecting an outsourcing service provider which has access to customer information. 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. For more details on due diligence, please refer to Section 5 "How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing" clause "9.2, 9.3 Assessment of service provider".
12.3	Customer data protection	12.3 FSPs must be satisfied that the OSP has in place policies, procedures and controls that are comparable to that of the FSPs, to ensure that customer information is properly safeguarded at all times.	Customers should ensure that the outsourcing service provider has established policies, procedures and control measures for protecting customer information. Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. To implement personal information protection and management, Tencent Cloud has established personal information management policies and procedures. These are designed to process personal information generated by customers during registration, purchase, and use of cloud services in accordance with the principles of legality, legitimacy, and minimal necessity.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			They also empower customers to manage their data and fulfill privacy protection obligations through various tools and services. The relevant policies and procedures specify requirements for the collection, use, storage, disclosure, restriction of processing and deletion of personal information, the concept of privacy by design, the handling of customer personal information after service termination, and the exercise of customer rights.
12.4 、 12.6	Service Level Agreement (SLA)	12.4 In ensuring the obligation to safeguard customer information is adequately reflected in a Service Level Agreement (SLA) with an OSP, at a minimum, the SLA must require the OSP to (a) undertake to safeguard the customer information and prevent any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means, of the customer information; (b) ensure the adequacy and effectiveness of its policies and procedures to protect the FSP's customer information; (c) conduct robust vetting on its personnel who handles customer information; (d) only allow its personnel to have access to customer information strictly for the purpose of carrying out the OSP's functions under the SLA; (e) ensure that its personnel understands and undertakes to comply with the prohibition on	Customers should sign a service level agreement and a confidentiality agreement with the outsourcing service provider, stipulating the obligations of the service provider to protect the customer's information. As a cloud service provider, Tencent Cloud offers online legal documents on its international portal such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, the service term, and the scenarios under which the agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud 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. For security incidents that may affect customers,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		disclosure by whatever means of customer information to any person for any purpose other than that which is specified in the SLA, permitted under the written law or approved by BNM, as the case may be (including after the end of the contract term); (f) investigate any customer information breach to determine when and how the breach occurred; (g) report any customer information breach to the FSP within an agreed timeframe; (h) destroy in accordance with paragraph 10.32 or return all customer information to the FSP upon the expiry or termination of the SLA; and (i) allow the FSP to audit or inspect how customer information is safeguarded. 12.6 FSPs must require the OSP to sign a binding non-disclosure undertaking with regard to the handling of customer information.	Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. Tencent Cloud will, as appropriate, assign dedicated personnel to actively respond to and support audit and supervisory requirements from customers.
12.7	Personnel training	12.7 FSPs must ensure that the OSP conducts training to its personnel, at regular intervals, on relevant policies and procedures relating to the proper handling of customer information as well as reviews the adequacy and effectiveness of the training programme.	Customers should ensure that the outsourcing service provider regularly conducts training for its staff on handling customer information and review the adequacy and effectiveness of the training plan. Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering

No.	Domain	Summary of Controls	Tencent Cloud's Response
			topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.
			Customers should conduct a review of the outsourcing service provider at least every two years to confirm that the provider is fulfilling its responsibilities and obligations regarding the protection of customer information in accordance with the terms of the contract.
			To comply with customers' outsourcing oversight requirements, Tencent Cloud will cooperate with third-party security audits and supervisory reviews in accordance with applicable agreements and provide dedicated assistance to actively support customer-initiated audit activities.
12.9	Regular review	12.9 FSPs must conduct a review of the OSP at least once in every two years to confirm that the OSP fulfils its obligations in accordance with the contract provisions in safeguarding the FSPs' customer information.	The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual independent professional audits by domestic and international third parties. Through System and Organization Controls (SOC) reports, Tencent Cloud provides assurance to cloud customers, independent auditors, regulators, shareholders, and other stakeholders regarding its latest internal control status.

07

How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Data Management and MIS Framework

Bank Negara Malaysia expects financial institutions to establish and maintain a sound data management and management information system (MIS) framework which to manage data and disseminate information throughout an organization effectively and efficiently provides a strong foundation for well-run financial institutions. Therefore, BNM released the [Guidelines on Data Management and Management Information System \("MIS"\) Framework for Development Financial Institutions \("DFI"\)](#) in 2011. This document outlines high-level guiding principles for sound data management and management information system practices, requiring financial institutions to establish robust, accurate, and secure management information systems. Financial institutions should structure and implement data and management information systems in a manner that is consistent with the principles set out in the Guidelines and appropriate to each institution's specific business needs.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in Guidelines on Data Management and Management Information System ("MIS") Framework for Development Financial Institutions ("DFI"), and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.10	Change management	4.10 Policies and procedures, including the appropriate approving authority, for effecting changes to data systems should be clearly defined. The policies and procedures should appropriately reflect the significance of specific data systems to critical business functions, with more rigorous controls entrenched for mission-critical systems.	Customers should formulate policies and procedures for data system changes and should adopt more stringent measures for system changes based on the importance of the data system to critical business functions. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also maintains an emergency change management process, under which emergency changes must receive appropriate approval before execution. All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conduct regular log

No.	Domain	Summary of Controls	Tencent Cloud's Response
			reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment. Tencent Cloud classifies change requests based on attributes such as importance, urgency, and scope of impact. For changes that may affect external environments—such as product, infrastructure, or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels.
4.12	Third party vendors	4.12 Where data is managed by third party vendors under outsourcing arrangements, senior management must ensure that effective oversight, review and reporting arrangements are established to ensure that service level agreements regarding standards on data quality, integrity and accessibility are observed at all times.	If the data is managed by a third-party vendor, customers should establish effective monitoring, review and reporting mechanisms to ensure compliance with the terms stipulated in the service level agreement. On Tencent Cloud international portal, Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization.
			Customers should establish a management mechanism for access control, effectively managing the logical and physical access to the system and data, ensuring that only authorized personnel can have access.
			To assist customers in implementing logical access control for the system and data, Cloud Access Management (CAM) helps customers
			securely and granularly manage access to Tencent Cloud products and resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions.
			To support regulatory compliance, Tencent Cloud has also established internal access control authorization policies and a role-separation matrix. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud uses a zero-trust security management system to authenticate employee access, requiring users to complete two-factor authentication through the system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions to employees only based on job responsibilities and business necessities. Regular permission reviews are conducted to prevent permission misuse and abuse.
			Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities.
4.20 、 4.23	Access controls	4.20 Financial institutions must establish adequate preventive and detective controls to ensure that logical and physical access to systems and data is secure and only available to authorised personnel for specific purposes. 4.23 Access rights to systems and data should be clearly defined, documented and where appropriate, segregated to prevent critical data or systems from being compromised. Given the sensitivity of the bulk of data handled by financial institutions, access should generally be given on a “need to know” basis.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud's internal office network is completely isolated from the production environment where customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-factor authentication. Tencent Cloud employs fine-grained permission management during authorization, granting employees only the minimum operational permissions and time limits necessary to provide services. All backend operational records are centrally stored in a logging platform and regularly reviewed by Tencent Cloud's internal audit team. All backend maintenance operations are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team conducts regular reviews of these records. For physical access control, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas.
4.21	Data classification	4.21 The controls should be commensurate with the criticality and sensitivity of the relevant systems and data handled. In this connection, policies and procedures should be established for the classification of data, having regard to the potential impact	Customers should establish policies and procedures for data classification, categorizing the data based on the potential impact of unauthorized access or tampering. The <u>Data Security Governance Center (DSGC)</u> helps customers automatically identify and classify cloud-based data assets and assess associated security risks. DSGC is an integrated data security operations platform that supports

No.	Domain	Summary of Controls	Tencent Cloud's Response
		that unauthorised access to, or tampering of, data could have on the institution's ability to accurately assess its risk exposures and financial condition, plan and manage its financial resources, preserve individual (including customers') rights to privacy, maintain the institution's competitive position, and fulfill its regulatory reporting obligations.	sensitive data discovery, classification and grading, data mapping, and abnormal access analysis. It works in coordination with Tencent Cloud's security capabilities to form a closed-loop data protection framework, maximizing security effectiveness for enterprises. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. To support customers in meeting regulatory requirements, Tencent Cloud has established data security management procedures that define principles for data classification and protection. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees do not attempt to access any customer data unless required for service delivery and explicitly authorized by the customer.
4.22	Critical data systems	4.22 Similarly, financial institutions should identify critical data systems, generally defined as those systems that, if disrupted or tampered with, would materially impact the institution's business operations, reputation or financial condition. More rigorous controls should be in place for access to data and systems classified as highly sensitive or critical.	Customers should identify the critical data systems based on the significant impact that service and functionality disruptions of the business have on the company's operations, reputation and finances. And customers should implement stricter access control for such systems. To support the Customer in meeting regulatory requirements, Tencent Cloud conducts business impact analysis for its cloud products and services in accordance with its internal business continuity management policies. This analysis includes identifying critical products and services, mapping activities that support service delivery, assessing the impact of disruptions over time,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			establishing recovery priority timelines at the minimum acceptable level, identifying dependencies and supporting resources, and formulating appropriate response strategies based on the analysis results.
4.24	Access log	4.24 Employees should not have concurrent access to data files residing in and computer facilities supporting both the production systems and backup systems. Persons given access to backup files or system recovery resources should be limited and duly authorised to have access for specific purposes and a specified period only. Any access should be documented and logged for audit purposes.	Customers should ensure that its employees do not have access to both the data files in the production system and the supporting computer facilities, as well as the backup system. The access rights to the backup files should have a limited duration. And it is necessary to ensure that all access activities are recorded in logs. Customers can use Cloud Access Management (CAM) to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. If customers encounter any issues related to accounts, network security, or product usage, they can submit a support ticket through the console to obtain technical assistance. Tencent Cloud provides a comprehensive operational security framework to ensure that service teams cannot directly access customer information assets without explicit customer consent and authorization. To support regulatory compliance, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the IT security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
4.25	Access to critical data or systems by external parties	4.25 Access to critical data or systems by external parties (e.g system vendors and service providers) must be properly authorised. Financial institutions must ensure that such access by external parties is closely supervised, monitored and appropriately restricted in line with the purpose of the access given. Legal agreements for services contracted should clearly prohibit the unauthorized disclosure of confidential data by the external party and provide for adequate remedies to the financial institution.	Customers should ensure that the access of external parties to critical data or systems is authorized appropriately, and that such access is supervised and monitored. Additionally, a legal agreement should be signed with the external party to explicitly prohibit the unauthorized disclosure of confidential data by the external party. Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the protection of user data and intellectual property, as well as confidentiality obligations. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related

No.	Domain	Summary of Controls	Tencent Cloud's Response
			to criminal incidents).
			Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities. Tencent Cloud's internal office network is completely isolated from the production environment where customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-factor authentication. Tencent Cloud employs fine-grained permission management during authorization, granting employees only the minimum operational permissions and time limits necessary to provide services. All backend operational records are centrally stored in a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
4.27	Personal data protection	4.27 Appropriate safeguards should be put in place to ensure that personal data is not misused or disclosed in a wrongful manner. Personal information (of customers, employees or any other parties that the financial institution may conduct business with) should be handled properly to ensure confidentiality of the information and compliance with relevant legislation.	Customers should establish an information protection mechanism to ensure that personal data is not misused or leaked, and to safeguard its confidentiality. To assist customers in complying with regulatory requirements, Tencent Cloud provides an online Privacy Policy, which clearly states that Tencent Cloud will process data in accordance with applicable laws and regulations both in the course of providing Tencent Cloud services and under any other circumstances. On this basis, Tencent Cloud regards personal data compliance as a top priority in the service provision process and adopts universally recognized personal data compliance principles (such as legality, fairness, transparency, purpose limitation, data minimization, integrity, accuracy, confidentiality,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and accountability) as the guiding philosophy for privacy compliance. These principles are integrated into all stages of product design and development as well as the entire lifecycle of personal data, making privacy compliance an inherent attribute of the products. 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.
4.28	Information Security Management Systems (ISMS) certification	4.28 To ensure that safeguards and security measures implemented over data and IT systems are effective, financial institutions are encouraged to obtain the MS ISO/IEC 27001:2007 Information Security Management Systems (ISMS) certification for critical systems, particularly the payment and settlement systems.	Customers should ensure the security of critical systems, especially the payment and settlement systems, and obtain the ISO27001 information security management system certification. Tencent Cloud has obtained the ISO/IEC 27001 certification through independent third-party audits or assessments. Obtaining the ISO 27001:2022 certification can better demonstrate Tencent Cloud's commitment to security, indicating that Tencent Cloud has established a scientific and effective management system and can provide users with secure and reliable cloud products and services.

08

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

Operational resilience of financial institutions is critical to ensure continuity in the provision of financial services through periods of disruptions, maintain orderly market conditions and sustain public confidence in the financial system. Bank Negara Malaysia issued the [Business Continuity Management](#) guidance in 2022, aiming to promote financial institutions to establish a robust business continuity framework, system, and processes in line with their overall risk appetite, and to strengthen sound risk management practices. This guideline aims to strengthen the capacity and preparedness of financial institutions to respond and recover from operational disruptions and preserve the continuity of critical business functions and essential services within a specified timeframe in the event of an operational disruption. The requirements mainly focus on areas such as risk assessment, business impact analysis, maximum tolerable downtime (MTD) and recovery time objective (RTO), recovery strategy, business continuity plan (BCP) and disaster recovery plan (DRP), crisis communication, alternate site and recovery site and testing and exercises.

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 and extracts the control requirements relevant to cloud service providers as outlined in Business Continuity Management, and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.1	Risk assessment	9.1 A financial institution must undertake RA to identify potential risks that may cause business disruptions and result in the financial institution not being able to fulfil its business obligations, and assess the likelihood of the occurrence of these threats.	Customers should conduct a risk assessment to identify potential risks that could lead to business disruption, and evaluate the likelihood of such threats occurring. Tencent Cloud conducts risk assessments for cloud products and services based on its internal business continuity management regulations. The main contents of risk assessment include: Identify business continuity-related resources and their values, identify threats to business continuity resources, identify the vulnerability of resources, comprehensively analyze the possibility of various threats and quantitatively or qualitatively describe the impact, and objectively evaluate the effectiveness of existing risk prevention and control measures.

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.3、9.5	Business impact analysis	9.3 A financial institution must also undertake BIA to assess the potential impact of various disruption scenarios to the financial institution.	Customers should conduct a business impact analysis to assess the potential impact of the disruption on the business.
		9.5 In performing the BIA, a financial institution must assess the financial and nonfinancial impacts to the financial institution due to the unavailability of critical business functions, resources and infrastructure during a disruption for a specific period of time, including prolonged periods as a result of high absenteeism or movement restrictions.	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.
9.7	Critical business functions	9.7 Based on the outcome of the RA and BIA, a financial institution must identify its CBFs and establish priorities for recovery	Customers should determine the priority of business recovery, recovery strategies, and resource allocation based on the criticality of business services and functions. To support the Customer in meeting regulatory requirements, Tencent Cloud conducts business impact analysis for its cloud products and services in accordance with its internal business continuity management policies. This analysis includes identifying critical products and services, mapping activities that support service delivery, assessing the impact of disruptions over time, establishing recovery priority timelines at the minimum acceptable level, identifying dependencies and supporting resources, and formulating appropriate response strategies based on the analysis results.
9.10-9.13	Maximum tolerable downtime (MTD) and recovery time objective	9.10 Based on the RA and BIA performed, a financial institution must determine the business continuity objectives for CBFs that correspond to varying levels of disruption as	Customers should set the Maximum Tolerable Downtime (MTD) and Recovery Time Objective (RTO) for each critical business function. For business functions that have a significant impact on customer service, shorter MTD and RTO should be set. Additionally, customers should

No.	Domain	Summary of Controls	Tencent Cloud's Response
	(RTO)	defined in paragraph 10.2. The business continuity objectives, which include the MTD and RTO, must - (a) be consistent with the overall risk appetite and risk management framework of the financial institution; (b) commensurate with the nature, scale and complexity of business functions and the inter-dependencies between functions; (c) correspond with the importance and criticality of the business functions; and (d) include procedures and the minimum level of resources required to recover the CBFs within the MTD and RTO. 9.11 A financial institution must set shorter MTD and RTO for business functions that have significant impact on customer services such as those listed in paragraph 9.14. 9.12 In determining the MTD and RTO, a financial institution must ensure that: (a) RTO does not exceed MTD; and (b) MTD and RTO facilitates the prompt recovery of essential services and CBFs that pose systemic impact to financial stability. 9.13 A financial institution must maintain proper documentation of business	properly keep the business continuity objectives and provide them when requested by the Bank. To ensure continuous availability of Customer operations, Tencent Cloud performs business impact analysis for its cloud products and services, defines RTOs and Recovery Point Objectives (RPOs), and develops response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans are established for cloud products and critical processes, covering facilities, personnel, equipment, systems, information and data, and business priorities.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		continuity objectives internally, which is to be made available to the Bank upon request.	
9.15	Essential services	9.15 To ensure continued availability of the essential services, a financial institution must have in place contingency arrangements to provide these essential services during a disruption and incorporate these arrangements in the BCP. This includes services which are performed by service providers on behalf of the financial institutions under outsourcing arrangements.	Customers should formulate contingency arrangements to ensure that essential services can be provided during the interruption period and incorporate this plan into their business continuity plan. Customers should also ensure that the contingency arrangements also cover the services provided by the service provider. To ensure business continuity for customers, Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud computing environment and has obtained international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud conducts Business Impact Analysis (BIA) for its cloud products and services to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Based on BIA results, Tencent Cloud develops appropriate strategies and business continuity plans, including detailed disaster recovery plans for cloud products. Tencent Cloud regularly performs business continuity drills and tests to validate the feasibility of these plans and procedures.
9.18	Recovery strategy	9.18 A financial institution must have in place a comprehensive recovery strategy that encompasses: (a) recovery objectives that take into account its risk appetite and nature, scale and complexity of its business operations; (b) recovery priorities that correspond to the recovery objectives and criticality of its	Customers should formulate a comprehensive business continuity plan (BCP) and disaster recovery plan (DRP), clearly defining the organizational structure, personnel roles and responsibilities, procedures for responding to business disruptions, communication procedures, resource list, and backup locations, etc. of the business continuity management plan. Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud computing environment and has obtained international

No.	Domain	Summary of Controls	Tencent Cloud's Response
		business functions;	certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud conducts Business Impact Analysis (BIA) for its cloud products and services to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Based on BIA results, Tencent Cloud develops appropriate strategies and business continuity plans, including detailed disaster recovery plans for cloud products. Tencent Cloud regularly performs business continuity drills and tests to validate the feasibility of these plans and procedures.
		(c) maximum time for recovery for its essential services, including MTD and RTO;	
		(d) adequacy and capability of infrastructure to support recovery (including functional relocation, alternate site and recovery site, modes of processing, work area, data and facility); and	
		(e) adequacy and capability of staff to support recovery (including recovery staff and decision makers).	From a personnel perspective , Tencent Cloud defines roles and responsibilities for recovery processes and implements an A/B role redundancy mechanism for critical skills and positions. Regular emergency drills and training are conducted to ensure rapid and effective execution of recovery procedures, supporting Customers in achieving timely restoration during business disruption scenarios.
9.21	business continuity plan (BCP) and disaster recovery plan (DRP)	9.21 For purposes of paragraph 9.20, the BCP and DRP must include– (a) governance, processes and criteria to activate the BCP and DRP; (b) roles and responsibilities of the BCM function and recovery staff, including their alternates; (c) procedures to be followed in response to a disruption to business operations, in order to respond swiftly to a crisis situation, recover or resume CBFs, resources and infrastructure within the stipulated timeframe; (d) escalation, declaration and notification procedures, including call trees and contact lists; (e) a list of all resources required to recover CBFs in the	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		event of a disruption. This would include, but is not limited to, key recovery staff, systems, computer hardware and software, office equipment and relevant documentation; (f) relevant information about the alternate site and recovery site; and (g) procedures for restoring normal business operations. This would include, but is not limited to, orderly entry of all business transactions and records into relevant systems and completion of all verification and reconciliation procedures.	
9.22	Crisis management plan (CMP)	9.22 A financial institution must also develop a CMP5 to guide and support the decision making by the CMT. The CMP must include the following: (a) the governance, processes and triggers to activate the CMT; (b) the roles and responsibilities of the CMT members; (c) identification of key internal and external stakeholders and their expected roles and involvement in managing a crisis; (d) methodology to be used by the CMT to assess impact of a crisis and guide actions to be taken (including ensuring staff safety, incident containment, evacuation and other crisis	Customers should establish frameworks, plans and procedures for crisis management, including communication strategies and channels with internal and external stakeholders, methodologies for assessing crisis impacts, standards for initiating business continuity plans, and response measures, etc. To support regulatory compliance, Tencent Cloud has developed crisis management procedures that define crisis levels and specify the processes and responsibilities for crisis prevention, analysis and handling, recovery, and post-crisis improvement. Tencent Cloud has also implemented an incident escalation mechanism to clarify communication paths and responsibility allocation during incidents, improving response efficiency and minimizing potential losses caused by unexpected events. For security incidents that may affect external Customers, Tencent Cloud has established incident reporting mechanisms and multiple communication channels to ensure timely

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management procedures); (e) clear criteria for activation of BCP, DRP and alternate site; (f) clear process on— (i) information gathering and status update to the CMT; (ii) timely internal and external communications; and (iii) supporting the CMT's oversight on the recovery and restoration efforts; (g) proper records of decisions made during a crisis; and (h) potential responses in the event that the duration of a crisis is prolonged.	notification to affected parties.
9.24	Outsourcing arrangements	9.24 A financial institution must ensure that its CMP, BCP and DRP provide for all outsourcing arrangements and comply with the relevant requirements in the policy document on Outsourcing.	Customers should ensure that their business continuity plan, disaster recovery plan and crisis management plan cover all outsourcing arrangements and comply with the relevant requirements stipulated in the outsourcing policy. To ensure business continuity for customers, Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud computing environment and has obtained international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud conducts Business Impact Analysis (BIA) for its cloud products and services to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Based on BIA results, Tencent Cloud develops appropriate strategies and business continuity plans, including detailed disaster recovery plans for cloud products. Tencent Cloud regularly performs business continuity drills and tests to validate the feasibility of these plans and procedures.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			For more details on outsourcing, please refer to Section 5 " How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing ".
9.25	Contractual and outsourcing arrangements	9.25 To enhance the effectiveness of BCM, a financial institution must incorporate the following requirements and clauses in contractual and outsourcing arrangements with key service providers, suppliers and counterparties: (a) require the key service provider, supplier and counterparty to have in place sound and effective BCP for the outsourced arrangement, including specific MTD and RTO requirements that align with the financial institution's MTD and RTO, and provisions for legal liability if MTD or RTO requirements are not met; (b) require the key service providers to participate in the financial institution's integrated testing, as stipulated in paragraph 9.50(d); (c) allow the internal audit of the financial institution or other independent party appointed by the financial institution to review the BCM of the key service provider, supplier and counterparty; and (d) allow the financial institution to have access to all relevant records and information maintained by the key service provider, supplier	Customers should incorporate the requirements of business continuity management into the contracts and outsourcing arrangements with key service providers, such as requiring the providers to establish and maintain effective business continuity plans, having key service providers participate in the integration tests, allowing financial institutions to audit their business continuity plans, and obtaining relevant records and information. Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, achieving ISO/IEC 22301 certification for its BCM system. To ensure service availability, Tencent Cloud regularly conducts business impact analyses for cloud products and services, defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and develops contingency strategies and continuity plans based on analysis results. Regular drills are conducted to validate plan effectiveness. If the customer assesses that the disaster recovery drill requires Tencent Cloud's participation and collaboration, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and counterparty with respect to the outsourced arrangement.	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.
9.26-9.27	Reviews and validations	9.26 A financial institution must have in place processes to perform periodic reviews, validations and updates on the components of its BCM framework to ensure their continued relevance and effectiveness towards the evolving changes in the operating environment, business activities and risks, and to address gaps identified from testing exercises. 9.27 In the event of an operational disruption, a financial institution must conduct a post-event review on the effectiveness of its CMP, BCP and DRP. The report must be communicated to the board and senior management for actions to be taken to address any identified gaps.	Customers should conduct regular reviews, validations and updates of each component within the business continuity management framework, and address the issues identified during testing. Additionally, if an operational disruption occurs, customers should assess the effectiveness of its business continuity plan and disaster recovery plan, and report the assessment results to the management. To support regulatory compliance, Tencent Cloud conducts an annual assessment of the completeness, adequacy, and effectiveness of its business continuity management system and revises the system based on the assessment results. Tencent Cloud also reviews its business continuity plans annually and updates them as necessary. When significant changes occur in business functions or critical resources, Tencent Cloud reviews the scope of critical services and their component dependencies and promptly revises the business continuity plans. Tencent Cloud has established continuous improvement procedures and mechanisms that define corrective, preventive, and improvement actions after an incident occurs. Tencent Cloud analyzes the actual or potential causes of incidents or issues, evaluates the need for corrective and preventive measures, identifies improvement opportunities, and implements approved actions. For incidents that result in operational disruption, Tencent Cloud's quality

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management department organizes a post-incident review with the responsible teams, summarizes lessons learned, and issues an incident investigation report. The quality management department monitors the implementation of subsequent improvements to prevent recurrence of similar incidents.
9.29-9.30、9.32-9.33	Crisis communication	9.29 A financial institution must formulate a crisis communication strategy and a crisis communication plan, which is incorporated in its CMP. 9.30 In the crisis communication plan, a financial institution must include— (a) a list of all relevant internal and external stakeholders that the financial institution plans to communicate with, in the event of a crisis, and the corresponding prioritisation and timeline of the communication; (b) designated contact person(s) to lead the communication with internal and external stakeholders; (c) broad messages that will be included in the communication statements to the different internal and external stakeholders based on the different disruption scenarios; (d) the appropriate communication protocol that must be adhered to; and (e) the communication channels, including the	Customers should formulate a crisis communication strategy and plan, which should include a list of internal and external contacts, key communication information, communication channels, and communication protocols, etc. To assist Customers in fulfilling communication and notification obligations, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses. Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		alternative channels that can be used when the primary communication channel is unavailable.	ensuring timely handling of Customer requests.
		9.32 A financial institution must ensure that its crisis communication provides clarity to its stakeholders on the business continuity and recovery actions that would be taken to restore the CBFs and essential services.	Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.
		9.33 A financial institution must establish a communication protocol which include–	
		(a) the nature and content of information to be shared with each stakeholder; and	
		(b) the classification of the sensitivity of information to be shared with each stakeholder, consistent with the information security classification of the financial institution.	
9.37 、 9.38	Alternate site and recovery site	9.37 A financial institution must set up its alternate site and recovery site that can be used if the business premise, infrastructure or systems supporting the CBFs become unavailable in the event of a disruption. 9.38 For purposes of paragraph 9.37, examples of an alternate site and a recovery site include in-house arrangements, or available through agreement with service providers, or a combination of both options.	Customer should establish alternate site and recovery site so that they can be put into use when the business sites, infrastructure or systems that support critical business functions are unavailable. To assist customers in meeting regulatory requirements, 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 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.
9.39 、 9.40	Suitability and capacity	9.39 A financial institution must assess the suitability and capacity of the alternate site and recovery site to ensure that the sites are– (a) sufficiently distanced from the primary site to minimise the risk of being affected by the same source of disruption; (b) using separate or alternative telecommunication network and power grid from the primary site to minimise the risk of single point of failure; (c) readily accessible and available for occupancy, taking into consideration the logistic requirements within the recovery timeframe stipulated in the BCP and DRP; and	Customers should assess the suitability and capacity of the alternate site and recovery site, ensuring that they are at a sufficient distance from the primary site, using separate telecommunications network, meeting logistics requirements, and possessing complete technical and resource requirements. The recovery site should be compatible in terms of capacity and capability with the primary system, and the system and application software should be continuously updated to the latest version and be consistent with the configuration of the primary site. Tencent Cloud launched three data centers in Malaysia in 2026, offering a range of cloud computing services including cloud servers, cloud databases, and CDN. Customers can independently choose the location for storing and processing their data based on their business location and preferences. To ensure continuous availability of Customer operations, Tencent Cloud provides a wide range

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(d) functional and able to meet technological and resource requirements, and are commensurate with the criticality of the business functions. 9.40 For technology requirements, a financial institution must ensure that the IT systems and telecommunications network at the recovery site are— (a) compatible with the primary systems of the financial institution in terms of capacity and capability to adequately support the CBFs; and (b) continuously updated with the latest version of systems and application software to align with the system configurations of the financial institution, including hardware and software upgrades or modifications.	of cloud products and services—including computer, network, storage, database, container, middleware, and security services—all designed with high availability and supported by disaster recovery plans. Tencent Cloud builds or leases data centers in multiple global locations in compliance with relevant international standards and local security requirements. Tencent Cloud connects each availability zone to multiple network carriers, enabling cross-region network redundancy and reducing the impact of carrier-level outages. Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures. Similarly, Tencent Cloud's computer nodes adopt redundancy, and any faulty node is automatically removed by the scheduler in real time, ensuring service continuity for Customer workloads. Tencent Cloud offers Customers multi-region and multi-availability zone options to meet disaster recovery and service level requirements.
9.41	Alternate site or recovery site is managed or owned by a third party	9.41 Where the alternate site or recovery site is managed or owned by a third party, a financial institution must ensure its outsourcing arrangements are in accordance with the policy document on Outsourcing, particularly the following: (a) execution of a service level agreement (SLA) between the financial institution and the third-party provider to ascertain the level and type of services to be provided to the	Where the alternate site or recovery site is managed or owned by a third party, customers' outsourcing arrangement must comply with the requirements of the outsourcing policy document, such as signing a service level agreement, mitigating concentration risks, assessing the capacity and capability of the service provider in providing services, as well as their physical and logical access control, and continuously reviewing and monitoring the service level of the service provider. Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting

No.	Domain	Summary of Controls	Tencent Cloud's Response
		financial institution in order to safeguard the interest of the financial institution; (b) mitigation of concentration risks, where the alternate or recovery site provided, managed or owned by the third party will be utilised by several customers or to customers within the same locality or industry. In this regard, the SLA must specifically identify the conditions under which the alternate or recovery site may be used and specify how customers would be accommodated if simultaneous disruptions affect several customers of the service provider; (c) assessment of the capacity and capability of the service provider for use for a reasonably prolonged period; (d) adequacy of physical and logical access controls provided by the service provider to safeguard the alternate or recovery site; and (e) periodic test, continuous review and monitoring on the level and type of service provided and the risk mitigation measures maintained by the financial institution.	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 addressing concentration risk, Tencent Cloud operates data centers across multiple global regions, organized into regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. When launching instances, customers can select any Availability Zone within a designated Region deploying instances across independent Availability Zones safeguards applications against failures in a single location. Customers can flexibly deploy data and systems across different regions or availability zones according to business development needs and data security requirements, adopting suitable business continuity models to meet disaster recovery objectives. To enable effective monitoring and management of system performance, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services. In terms of physical access control, Tencent Cloud requires operators to verify the identity of personnel entering the data center, inspect and register the items they carry, and regularly review data center access permissions, promptly revoking access that is no longer relevant or unnecessary. In terms of logical access control, Tencent Cloud authenticates employees through a zero-trust security management system. Users must complete two-factor authentication via this system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting employees only the permissions necessary for their job responsibilities and business needs. Regular permission audits are conducted to prevent permission misuse and abuse. Tencent Cloud will provide dedicated assistance and actively cooperate with customers in audits and supervisory reviews as required.
9.42 、 9.43	Critical business information records	9.42 A financial institution must maintain and safeguard critical business information records that are crucial in providing essential services. 9.43 A financial institution	Customers should properly safeguard the critical business information that is essential for providing essential services and ensure that this information can be accessed at any time in the event of a disruption, so as to support the restoration of critical business functions.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		must have in place proper processes and controls to safeguard critical business information and ensure that they are readily accessible to facilitate recovery of CBFs in the event of a disruption.	Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customers' needs, such as: • <u>Cloud Object Storage (COS)</u>: Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS)</u>: Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS)</u>: Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C</u>: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL</u>: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB</u>: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios.
9.50 、 9.51 、 9.53	Testing and exercises	9.50 A financial institution must periodically conduct an integrated testing on a reasonable wide-scale basis for all the CBFs, including those undertaken by the key service	Customers should conduct regular integration tests, with the test scope covering the parts executed by the key service providers, ensuring that the key service providers participate in the tests. Additionally, when designing and implementing the tests, customers should

No.	Domain	Summary of Controls	Tencent Cloud's Response
		providers, commensurate with its size, nature, complexity and risk profile. In doing so, the financial institution must— (a) use backup IT systems to gauge and assess its application system linkages and network connectivity; (b) calibrate the load or capacity requirements that are required to support minimum service levels to be provided during a disruption; (c) include such calibrations in subsequent rounds of testing; and (d) ensure participation of key service providers to evaluate their adequacy and readiness to respond to the recovery measures, that the financial institution needs to deploy during a disruption. 9.51 In designing and carrying out the testing, a financial institution must— (a) develop test plans with predetermined test goals, scope and test evaluation criteria, using realistic simulations¹⁰ and activity volumes; (b) develop metrics to measure effectiveness of the BCP and DRP and the extent to which various business continuity objectives are met; (c) develop necessary contingency measures in the event of failed testing to avoid	formulate a test plan, keep formal test documents, compile post-test analysis reports, identify problems and specify rectification plans, and report the test results to the management. Customers can leverage the Tencent Cloud Smart Advisor (TSA) service to assist with planning and executing business continuity tests. This service is a cloud governance platform that integrates multiple ITOM vertical applications and draws on Tencent Cloud's extensive operational expertise. Through risk inspections, fault drills, and other governance measures, Cloud Advisor optimizes cloud infrastructure. For stress testing, Tencent Cloud provides Performance Testing Service (PTS), which simulates real business scenarios with massive user traffic to comprehensively validate system availability and stability. To support regulatory compliance, Tencent Cloud regularly conducts drills and tests for emergency response and disaster recovery internally. Tencent Cloud performs risk assessments on the drill plans to avoid any negative impact on services due to the drills. Disaster recovery drills typically simulate real-world disaster scenarios, including attack-defense exercises and large-scale failures, to thoroughly assess system resilience, response speed, and recovery capability. After each drill, relevant departments prepare a detailed drill report, which is archived along with the drill plan. The report generally includes the drill objectives and scope, execution plan, participants, preparatory work, key processes and timelines, identified issues, corrective measures and implementation plans, and conclusions. For issues identified during drills, Tencent Cloud implements corrective actions and promptly updates corresponding emergency plans. The audit department monitors the implementation of these corrective actions to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		business disruptions; and (d) maintain formal testing documentation, including test plan, objectives, scenarios, procedures and results, for future reference and audit. 9.53 A financial institution must prepare a post-test analysis report to evaluate the testing outcomes against the testing goals. This is to ensure adequacy and integrity of testing, to identify problems and to develop the necessary corrective action plans. The test results and post-test analysis report must be communicated to the board in a timely manner and made available to the Bank upon request.	ensure 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.
10.5	Cyber incident	10.5 For all cyber incidents, a financial institution must notify the Bank within 2 hours upon the confirmation of the disruption.	Customers should ensure that all cyber incidents are reported to the Bank Negara Malaysia within two hours after the disruption is confirmed. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—<u>Cloud Security Center (CSC)</u>. Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the efficiency of security operations. Regarding incident communication and notification, Tencent Cloud has developed an information security incident management standard, which includes procedures for incident response, escalation, and notification. This ensures timely alerts or notifications to internal

No.	Domain	Summary of Controls	Tencent Cloud's Response
			personnel, customers, and other relevant parties who may be affected by an incident, enabling orderly, timely, and efficient communication and coordination. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. 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. 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.

09

How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Risk Management in Technology ("RMiT")

With prevalent use of information technology in the provision of financial services, the Bank Negara Malaysia (BNM) has released the [Risk Management in Technology \("RMiT"\)](#), providing guidance for financial institutions to invest in the required expertise and risk controls to prevent operational disruptions given the complexity of IT systems, and maintain robust oversight to prevent transmission of risks with increased third party interlinkages. This policy document sets out the Bank's policy objectives and minimum requirements to improve financial institutions' management of technology risk, including cyber risk. In applying this policy document, a financial institution shall have regard to the size and complexity of its operations, the level of technology use and its external stress exposure to adopt risk controls that commensurate with the increased technology risk exposure of the institution. The requirements mainly focus on areas such as Technology Operations Management, Cybersecurity Management, Technology Audits, External Party Assurance, Internal Awareness and Training and Key Risks and Control Measures for Cloud Services.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in Risk Management in Technology ("RMiT"), and explains how Tencent Cloud, as a cloud service provider, assists financial institutions in complying with these requirements.

9.1 Technology Operations Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.4-10.11、10.14	System Development and Acquisition	10.4 A financial institution must establish a framework to guide the design, planning, implementation and governance of an enterprise technology architecture. A technology architecture serves as a foundation on which financial institutions plan and structure system development and acquisition strategies to meet business goals. 10.5 A financial institution must adopt a methodology for an effective and secure implementation of IT systems. Key phases of System Development Life Cycle (SDLC) shall include requirement, design, development, testing, deployment, change management, maintenance and	Customers should establish a security development management mechanism, clearly defining the security requirements for the system development life cycle (including requirements, design, development, testing, deployment changes, etc.). This includes conducting IT security compliance reviews, formulating system testing methodologies, protecting system test data, conducting source code reviews, establishing coding standards, and isolating test environments from production environments. Additionally, automated tools should be used to achieve timely security assessment of critical systems. Customers can leverage Cloud Native Build (CNB), which is deeply integrated with agile development concepts. From issues and merge requests to task sets, CNB provides a structured agile workflow, enabling customers to validate product iterations quickly and cost-effectively before market release. CNB provides a complete developer toolchain, including code hosting, high-performance CI/CD pipelines, AI code

No.	Domain	Summary of Controls	Tencent Cloud's Response
		decommissioning.	assistant, and artifact management. The AI code assistant, designed specifically for developers, supports multiple mainstream programming languages and offers features such as code completion, unit testing, code diagnostics, intelligent reviews, and smart Q&A for code issues—helping developers improve coding quality and efficiency.
		10.6 A financial institution must meet enterprise security, governance and compliance requirements when using rapid system development methodology. Given the dynamic environment can increase likelihood of errors, a financial institution shall automate the IT security compliance review to prevent unauthorised access as well as the discovery, remediation and testing of security vulnerabilities to ensure secure release of new IT services.	Tencent Cloud embeds essential SDLC principles and Security-by-Design concepts throughout its agile development process. The secure product development lifecycle incorporates information security and privacy protection across all stages—requirements analysis, design, development, testing, delivery, and operations—ensuring robust security controls throughout the product lifecycle. Key security measures include:
		10.7 A financial institution shall segregate the production environment from the development and testing environment to mitigate risk unauthorised changes to the production systems. Where a financial institution is relying on a cloud environment, the financial institution shall ensure that these environments are not running on the same virtual host.	• Security Training: Promoting secure coding awareness among developers and enforcing strict adherence to secure coding standards. • Requirements Analysis: Security integration is considered during business process and technical framework discussions. • System Design: Threat modeling and security assessments are performed on system architecture.
		10.8 A financial institution must establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, the financial institution must ensure proper authorisation procedures and adequate	• System Development: Tencent provides secure development components for use during coding, following Tencent Cloud's secure coding guidelines. • Security Validation: Vulnerabilities are identified through code security checks, asset scans, web scans, manual security assessments, penetration testing, and code audits. • Release: Only after all high-risk issues have been fixed can the system be released

No.	Domain	Summary of Controls	Tencent Cloud's Response
		measures to prevent their unauthorised disclosure are in place.	to production to prevent vulnerabilities from being introduced into live environments.
		10.9 The scope of system testing referred to in paragraph 10.8 may include unit testing, integration testing, user acceptance testing, application security testing, stress and load testing, and exception and negative testing, where applicable.	Tencent Cloud's change and release management process covers changes to applications, configuration files, operating systems, and databases. All changes must undergo independent functional testing before deployment. After implementing changes, Tencent Cloud's business team performs critical path regression validation to ensure changes meet expectations and do not introduce abnormal behaviour or performance degradation, thereby maintaining overall system stability and availability. Furthermore, Tencent Cloud ensures that the development/testing environment and the production environment are isolated from each other, and prohibits the use of unsensitized production data in the development/testing environment.
		10.10 A financial institution must ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure code is secure and was developed in line with recognised coding practices prior to introducing any system changes.	
		10.11 A financial institution must establish appropriate procedures to independently review and approve system changes. The financial institution must also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimise any business disruption.	
		10.14 A financial institution shall deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to facilitate timely security assessment of critical systems in keeping with	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		growing complexity in IT systems and emerging cyber threats.	
10.12、 10.15	Critical Systems Developed or Maintained by Third Party Service Provider	10.12 In relation to critical systems that are developed or maintained by third party service provider, a financial institution must, through contractual obligations, require third party service provider to: (a) provide sufficient notice to the financial institution before any changes are undertaken that may impact the IT system; (b) demonstrate that it adopts secure by design principles in IT system development methodology to mitigate cyber risks from propagating across the supply chain; and (c) ensure the source code continues to be readily accessible for business continuity. 10.15 Where third party software is used, a financial institution shall consider the potential risks and impacts a cyber supply chain incident may pose to its overall business operations and services. A financial institution shall consider, at the minimum: (a) adopting Software-Bill-of-Material (SBOM) to automate the identification and continuous monitoring of potential security vulnerabilities including security issues associated with	Customers use a third-party service provider to develop or maintain the critical system, they should require the third-party to notify promptly before making any changes that may affect the system, adopt a system development with secure by design principles, and ensure that the source code of the third-party is continuously accessible. In addition, when using third-party software, customers should adopt Software-Bill-of-Material automation to identify and monitor potential vulnerabilities and establish security policies and procedures for managing open-source software. Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud integrates the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System into the entire secure product development lifecycle. This approach covers all stages—requirements, design, development, testing, delivery, and operations—embedding information security and privacy protection principles throughout the product lifecycle to ensure robust security controls and assessments. For changes that may affect external environments—such as product, infrastructure,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		third party software components; and (b) establishing open-source software security policy and procedures. This includes ensuring secure access to source code repositories in third party platforms, regular monitoring to prevent data leakages, adoption of secure coding practices, robust testing of open-source software and timely vulnerability assessment to mitigate security vulnerabilities and propagation of malwares across supply chain.	or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels. For third-party product usage , Tencent Cloud has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies.
10.16	Asset Management	10.16 A financial institution must develop and implement robust policies to identify and reduce shadow IT risks.	Customers should ensure that all technology use and IT system development are managed within the framework of technical risk management, in order to reduce the risks associated with shadow IT. 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. Customers can also adopt Tencent Cloud's one-stop security management platform, Cloud Security Center (CSC), for information asset security management. CSC 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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.
10.17、 10.18	Patch and End-of-Life System Management	10.17 A financial institution must ensure that all systems including digital services are not running with known security vulnerabilities, on outdated platform or end-of-life (EOL) technology systems. In this regard, a financial institution must: (a) maintain current security baseline for the security hardening of technology components and ensure the security baseline is accurate and up to date; (b) continuously monitor and implement latest patch releases in a timely manner; (c) identify, plan and implement remedial action for technology systems that are approaching EOL; and (d) obtain management approval for any exception permitting the continued use of	Customers should establish a security baseline for the security hardening of technical components, continuous monitoring, timely implementation of the latest patches, conducting compatibility tests before patch implementation, and identifying technical systems that are about to reach the end of life to ensure that all systems do not run on those with known security vulnerabilities or those that have reached the end of life. In terms of security baseline and configuration management, Tencent Cloud's Cloud Security Center (CSC) provides automated configuration risk assessment capabilities to help customers reduce security risks caused by misconfigurations and improve overall cloud security posture. Customers can also use Config Audit to perform centralized auditing and governance of cloud resources, continuously recording configuration details and changes across different regions under their account. Based on Tencent Cloud best practices and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		unsupported or outdated technology. This exception must be substantiated by a thorough risk assessment with clear timeline for phasing out the outdated technology and are regularly reviewed at least on annual basis to ensure associated risks are effectively managed. 10.18 A financial institution must establish a patch and EOL management framework which addresses among others the following requirements: (a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems; (b) formulation of criteria, priority and turnaround time for patch deployment according to the severity of the vulnerabilities identified; (c) conduct of compatibility testing prior to the deployment of patches to minimise disruption to connected systems; (d) adherence to the workflow for end-to-end patch deployment processes including approval, testing, monitoring and tracking of activities; and (e) end-user awareness for orderly transition.	management of cloud resources. To support regulatory compliance, Tencent Cloud has established network security configuration standards and security baseline standards to standardize the configuration of network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud continuously scans operating systems, database management systems, and virtual images for deviations from established standards. When deviations are detected, Tencent Cloud automatically generates security tickets and assigns them to responsible teams for timely remediation. Tencent Cloud also conducts regular reviews of security policies and parameter settings for routers, firewalls, and network servers to ensure their effectiveness. For patch management, Customers can use <u>Cloud Workload Protection Platform (CWPP)</u> to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, receive real-time alerts, and obtain remediation plans to quickly address vulnerability risks. <u>Tencent Cloud Container Security Service (TCSS)</u> provides a virtual patching system designed to protect against frequently occurring zero-day vulnerabilities. It integrates Tencent's vulnerability discovery and real-time high-risk vulnerability alerting technologies to capture and analyse vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically apply them to cloud servers to effectively block hacking attempts. In addition, customers can use <u>Vulnerability Scanning Service (VSS)</u> to perform regular security scans on enterprise network devices and application services, receive continuous risk alerts and vulnerability detection, and obtain professional remediation recommendations to reduce security risks. Tencent Cloud identifies the latest patches and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Tencent Cloud also operates internal vulnerability scanning and external vulnerability reporting platforms to track and remediate issues. Security tickets are logged in the operations system and assigned to responsible teams for timely resolution. Tencent Cloud's security research team integrates virtual patching capabilities into its Web Application Firewall to enhance overall platform security. For technology End-of-life management, Tencent Cloud maintains a detailed inventory of hardware and facilities in its Configuration Management Database (CMDB), including each server's End-of-Support (EOS) date and version information. Tencent Cloud regularly retires and replaces servers, while software components (such as operating systems and database systems) are upgraded to appropriate versions before reaching end-of-support. For decommissioned hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction in official logs.
10.20-10.23	Cryptography	10.20 A financial institution must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. (a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation; (b) the adoption of robust and	Customers should establish a cryptography management policy, considering the adoption of recognized encryption algorithms in the industry. All encryption algorithms should undergo rigorous testing and evaluation to meet security goals and requirements. Customers should also implement a key lifecycle management mechanism and use certificates issued by dedicated certificate authority to manage the storage and transmission of keys. In terms of data storage encryption, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength cryptographic algorithms.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		secure processes in managing cryptographic key lifecycles; (c) the periodic review, at least annually, of all cryptographic standards and algorithms currently in use for critical systems, external linked or transactional customer-facing applications; (d) the expansion of IT asset inventory to include all cryptographic tools and algorithms in use with pertinent information on the rationale for each cryptographic method employed and its mapping to supported application systems; and (e) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. 10.21 A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Additionally, a financial institution must ensure the following: (a) except for non-critical systems or applications that do not contain customer data, the financial institution must retain ownership and control of the encryption keys to minimize	In terms of data transmission encryption, customers communications on the Tencent Cloud console are protected by the HTTPS security protocol. Tencent Cloud's cloud products provide API interfaces with HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations. If customers need to build their own applications on the Tencent Cloud platform, Tencent Cloud also offers a one-stop service for SSL certificates, including certificate application, management and deployment functions. It collaborates with top digital certificate authorization CA institutions and agents to provide HTTPS solutions for customers' websites and mobile applications. To help customers protect the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS). KMS enables customers to easily create and manage keys, meeting multi-application and multi-business key management needs while complying with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, allowing customers to apply encryption effortlessly. KMS supports external key import, allowing customers to use their own key material for encrypting and decrypting sensitive data on Tencent Cloud's architecture, thereby implementing a Bring Your Own Key (BYOK) solution on Tencent Cloud. KMS is built on FIPS 140-2 certified Hardware Security Modules (HSMs) for key generation and protection, uses secure data transmission protocols, and employs a multi-data-center distributed cluster architecture with hot backups. Underlying HSM devices are deployed with dual-site cold backups to ensure high availability of the key management system.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the risk of unauthorised access to the data; (b) where the financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys securely including adhere to relevant industry standard; (c) where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance; and (d) the financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. 10.22 A financial institution must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols must be based on recognised	KMS supports regular key rotation. Rotated keys remain compatible with previously encrypted data, ensuring no impact on customer operations. KMS securely deletes expired, invalid, or compromised keys using irreversible methods, making deleted keys unrecoverable and rendering associated encrypted data permanently inaccessible. Tencent Cloud has also established internal encryption and key management standards, defining security requirements for key application, generation, storage, usage, transmission, rotation, and destruction. All key lifecycle operations follow strict controls, including dual authorization, secure handover, proper storage, and timely updates. During key usage, Tencent Cloud enforces segregation of duties, rigorous approval processes, and real-name operations, while maintaining detailed key operation logs and performing regular audits. Tencent Cloud also considers factors such as key purpose, sensitivity of protected data, likelihood and impact of compromise to manage keys throughout their lifecycle.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation must be undertaken in a protected environment, supported by a hardware security module (HSM), trusted execution environment (TEE) or similarly secured devices. 10.23 A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.24-10.28	Data Centre Resilience	10.24 A financial institution must specify the resilience and availability objectives of its data centres to effectively support its business recovery objectives.	Customers should ensure that the data center has redundant capacity components and multiple distribution paths, ensuring that the power, network connection, cooling system, and mechanical and electrical systems of the data center have sufficient redundancy to eliminate any single-point failures. Customers should implement necessary monitoring and access control measures for the data center to ensure its physical and environmental security, especially for critical systems, where dedicated space management can be considered.
		10.25 A financial institution must ensure data centres have redundant capacity components and multiple distribution paths serving the computer equipment to eliminate any single point of failure for effective achievement of the identified business recovery objectives.	As a cloud service provider, Tencent Cloud is committed to delivering secure, stable, continuous, and reliable physical infrastructure for customers. To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, organized by regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. Customers can flexibly deploy data and systems across different regions or availability zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures.
		10.26 A financial institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A financial institution must also ensure there is no single point of failure in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A financial institution must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues.	Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point device failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability.
		10.27 A financial institution	In 2026, Tencent Cloud launched three data centers in Malaysia. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering

No.	Domain	Summary of Controls	Tencent Cloud's Response
		must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions. 10.28 A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.	the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. For leased data centers in Malaysia, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity, Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the data center. For physical access control, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure

No.	Domain	Summary of Controls	Tencent Cloud's Response
			failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. For physical and environmental incidents, Tencent Cloud requires operators to establish escalation mechanisms, response plans, and handling procedures, and to conduct regular drills to validate these processes. This ensures rapid response and resolution of such incidents, minimizing their impact on Tencent Cloud's platform and services. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts annual on-site audits to verify that data center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures.
10.29、 10.30	Capacity management	10.29 A financial institution must ensure its system capacity needs are well-planned and managed with due regard to peak processing period, business growth plans and technology architecture changes. 10.30 A financial institution must establish real-time monitoring mechanisms to	Customers should continuously monitor the capable of system resources, set performance and capacity thresholds, and implement necessary procedures to manage situations that exceed the preset thresholds. To support customers in efficient capacity planning and adjustment, Tencent Cloud provides Auto Scaling (AS) services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing actionable alerts to administrators to enable timely detection and resolution of service interruptions. The monitoring scope, metrics and thresholds shall be updated periodically to ensure they remain effective.	policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. To enable effective monitoring and management of system performance, customers can use <u>Tencent Cloud Observability Platform (TCOP)</u>. This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.32- 10.35	Service Availability	10.32 For critical systems, where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that these systems are designed for high availability with a cumulative unplanned downtime affecting the interface with customers or counterparties of not more than 4 hours on a rolling 12 months basis and a maximum tolerable downtime of 120 minutes per incident.	Customers are required to ensure that disruption to essential services caused by technology failures or cyber incidents does not exceed 4 hours on a rolling 12-month basis and a maximum tolerable downtime of 120 minutes per incident. Moreover, when significant changes occur in the risk environment, the effectiveness of system design, emergency arrangements, and capacity management should be reviewed. Additionally, customers are expected to implement an incident response plan, and promptly and effectively communicate with stakeholders in the event of a security incident. Customers should assess whether their core systems excessively rely on a single technology vendor or identical technology architecture, and develop a technology diversification strategy.
		10.34 A financial institution shall prioritise diversity in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.	Tencent Cloud supports customers in building hybrid cloud and multi-cloud architectures by providing standardized APIs and data migration tools to reduce vendor lock-in risks. Furthermore, Tencent Cloud's underlying technology infrastructure utilizes diversified hardware vendors to avoid systemic risks associated with a single technology stack.
		10.35 During an interruption of digital services or delivery channels, including periods of performance degradation or intermittent failures, a financial institution shall respond promptly and effectively to minimise the impact on its customers. This includes but not limited to- (a) ensure timely escalation and decision-making to resume services promptly via alternative arrangements and stabilise performance within the timeframe specified in paragraph 10.32 under all	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. For incident detection and response , Tencent Cloud has established a detailed incident management process and uses an internal security operations system to record security incidents. Detected incidents are analysed and classified based on nature, data sensitivity, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		plausible scenarios;	impact scope, and relevant personnel are promptly notified for follow-up.
		(b) define clear accountabilities for managing performance degradation issues and formalise arrangements with third party service providers to ensure effective coordination and timely recovery to normal performance levels;	In terms of communication and notification of the incident , Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses.
		(c) establish a communication plan for service interruptions to immediately inform affected customers, properly manage a high volume of customer feedback, and provide frequent updates on recovery efforts, as well as actionable information on available alternatives for customers with urgent needs;	
		(d) provide customers with a convenient means of checking the availability of digital services, which may include publishing real-time availability and performance status of its digital services on the corporate website; and	Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests.
		(e) disclose the track record of service availability on a quarterly basis within 15 calendar days of quarter-end, beginning from 15 October 2027.	Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.36-10.43	Network Resilience	10.36 A financial institution must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.	Customers should design a reliable, scalable and secure enterprise network, and clearly define the physical and logical connection relationships among network components in the network design diagram and take necessary measures to ensure the reliability of critical system network services, as well as the confidentiality, integrity and availability of data, avoiding the impact of potential network failures and network threats.
		10.37 A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.	In addition, customers should monitor network devices and network bandwidth and keep network device logs for at least three years.
		10.38 The control measures to prevent from network faults as referred to in paragraph 10.37 are expected to include component redundancy, service diversity and alternate network paths.	Tencent Cloud connects each availability zone to multiple network carriers, enabling cross-region network redundancy and reducing the impact of carrier-level outages. Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures.
		10.39 A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.	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.
		10.40 A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	To meet network segmentation or zoning requirements , customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built
		10.41 A financial institution	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		must establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint must highlight both physical and logical connectivity between network components and network segmentations. 10.42 A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years. 10.43 A financial institution must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the financial institution from other entities within the group.	on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. In the aspect of network device log management, Customers may use Cloud Log Service (CLS), a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. The Cloud Security Center (CSC) aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis.
10.44 、 10.45	System backup and restoration	10.44 A financial institution must establish a robust backup strategy and procedures to meet business recovery objectives. At a minimum, a financial institution shall- (a) establish backup and restoration procedures to effectively manage the backup data life cycle; (b) maintain an adequate number of backup copies of all critical data, the updated version of the operating system software, production	Customers should establish a backup management mechanism to effectively manage the lifecycle of backup data, encrypt and physically protect the backup storage media, and conduct regular backup recovery tests. Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customer needs, such as: • Cloud Object Storage (COS): Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case

No.	Domain	Summary of Controls	Tencent Cloud's Response
		programs, system utilities, all master and transaction files and event logs for recovery purposes; (c) backup media must be stored in an environmentally secure and access-controlled backup site; (d) secure the storage and transportation of sensitive data in removable media to meet minimum controls as specified in Appendix 1 or equivalent; (e) test backup and restoration procedures periodically to validate recovery capabilities. Remedial actions shall be taken promptly by the financial institution to fix the root cause of unsuccessful backups; and (f) undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times. 10.45 A financial institution shall establish tamper-proof backup arrangement and an isolated recovery environment to enable timely resumption of essential banking and payment services within its tolerable level in the event of destructive cyber-attacks such as widespread data loss caused by ransomware.	of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS)</u>: Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS)</u>: Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C</u>: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL</u>: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB</u>: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios.

No.	Domain	Summary of Controls	Tencent Cloud's Response
10.47-10.49	Third Party Service Provider Management	10.47 A financial institution must conduct due diligence on the third party service prior its on-boarding or engagement and throughout the service engagement to ensure achievement of business performance and recovery objectives remain unimpaired, considering the latest risk environment.	Customers should conduct due diligence before the third-party service provider prior to its on-boarding or engagement and throughout the service engagement. When hiring the third-party service provider, a service level agreement should be signed. Additionally, customers should continuously monitor the cybersecurity posture of the third-party service provider and effectively manage security incidents.
		10.48 A financial institution must establish Service Level Agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following:	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.
		(a) access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution. This shall include access to any record, file or data of the financial institution, including management information and the minutes of all consultative and decision-making processes;	For more details on due diligence, please refer to Section 5 " How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing " clause " 9.2, 9.3 Assessment of service provider ".
		(b) requirements for the third party service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial;	Tencent Cloud provides online legal documents such as the Terms of Service , Service Level Agreement (SLA) , and Data Processing and Security Agreement . These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions.
		(c) a written undertaking by the third party service provider on compliance with secrecy provisions under relevant	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.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		legislation. The SLA shall further clearly provide for the third party service provider to be bound by integrity and confidentiality provisions stipulated under the contract even after the engagement has ended; (d) arrangements for disaster recovery and backup capability, where applicable; (e) critical system availability; (f) arrangements to facilitate an orderly exit in the event of exit or termination of the third party service provider, which includes ensuring data residing in third party service providers are recoverable in a timely manner; (g) responsibility of third party service providers to promptly disclose and notify the financial institution of any service disruptions or cyber incidents that affect financial institution or customer data that occur within the service providers' or sub-contractors' environment. This enables financial institutions to provide timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident; and (h) requirements for the third party service providers to comply with the relevant internationally recognised standards and ensure their key staff obtain the relevant	For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses. Tencent has established a Security Technology Committee and specialized security teams across different functions and domains, supported by an experienced industry expert service team dedicated to delivering secure, reliable, professional, and compliant products and services. Tencent Cloud has established robust HR management standards and procedures to ensure appropriate recruitment and placement based on job requirements. Background checks, including verification of education and certifications, are conducted during recruitment.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		certifications. 10.49 A financial institution must formulate a roadmap to achieve continuous monitoring of a third party service provider's cybersecurity posture to obtain real-time insights for effective incident management. The financial institution shall undertake the following: (a) measure the IT infrastructure footprint and the customer information accessible to third parties, and regularly manage this external stress state exposures to mitigate cyber-attack surfaces; (b) adopt leading security policies and controls to mitigate product-specific third party risks; (c) ensure incident response plans incorporate protocols with third party service providers to detect and contain adverse impact of security vulnerabilities resulting from software updates; (d) define a priority set of security controls that require more frequent assurance assertion from the third party service providers; (e) monitor technology and cyber incidents information disclosed by third party service providers at a higher frequency; (f) implement technology	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		solutions to automate metric testing; and (g) establish processes to respond to breached thresholds, including investigating failed assertions and remedying control gaps.	
10.50	Cloud Services	10.50 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment must specifically address risks associated with the following: (a) sophistication of the deployment model; (b) migration of existing systems to cloud infrastructure; (c) location of cloud infrastructure including potential geo-political risks and legal risks that may impede compliance with any legal or regulatory requirements; (d) multi-tenancy or data co-mingling; (e) vendor lock-in and application portability or interoperability; (f) ability to customise security configurations of the cloud	Customers should ensure proper management of the use of cloud services, ensuring that the governance and control levels implemented by the cloud service provider are commensurate with the risks associated with using cloud services. Additionally, customers should conduct a risk assessment when planning to adopt cloud services, covering at least cloud risk management, the geographical location of cloud infrastructure, multi-tenancy situation, identity and access control, data protection and key management, public cloud network security, cloud resilience management, portability, migration to the cloud, and compliance with applicable regulatory requirements. Tencent Cloud, in accordance with contractual agreements, grants customers audit and oversight rights and provides dedicated personnel to actively support customer-initiated audits or inspections. For migration of existing systems to cloud infrastructure, Cloud Migration(CMG) integrates various migration tools enables customers to quickly migrate system to the cloud. For location of cloud infrastructure, Tencent Cloud strictly complies with the laws and regulations of the jurisdictions in which it operates. Tencent Cloud's infrastructure is deployed across multiple global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an isolated fault domain with physical separation.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		infrastructure to ensure a high level of data and technology system protection; (g) exposure to cyber-attacks via cloud service providers; (h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination; (i) demarcation of responsibilities, limitations and liability of the cloud service provider; and (j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.	Customers can flexibly deploy data and systems across different regions or availability zones based on business growth needs and data security requirements to meet disaster recovery objectives. In terms of security configuration for customized cloud infrastructure, Tencent Cloud has tailored various solutions for multiple financial institutions, providing regulatory-compliant financial private cloud services to numerous customers, possessing financial-grade security and compliance capabilities. For tenant isolation, Tencent Cloud employs methods such as underlying resource virtualization isolation, network isolation, and data isolation to architecturally reduce the impact on customers in the event of an attack on the cloud service provider. 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. If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Tencent Cloud supports data migration using standard formats and the same transmission methods as during onboarding, including Direct Connect (DC) and VPN Connection, services, to ensure secure and reliable data transfer. Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud 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 undergoes professional third-party audits annually. For more detailed information about cloud services, please refer to Section 9.8 "9.8 Key Risks and Control Measures for Cloud Services".
10.52	Data protection	10.52 A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	Customers should assess and manage the IT systems and data in the cloud environment, ensuring that the cloud service provider takes necessary measures to protect data security and prevent unauthorized access and disclosure. For sensitive data, customers should establish an appropriate encryption key management mechanism. For data access and protection aspects, customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. For data storage security aspects, Tencent Cloud storage and database products support encryption using strong algorithms. Redundant storage and erasure coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			To assist customers in protecting the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS), which enables customers to easily create and manage keys for multiple applications and business scenarios in compliance with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, simplifying encryption implementation.
10.53-10.57	Access Control	10.53 A financial institution must implement an access control policy for the identification, authentication, and authorisation of all users to its IT assets and data. The level of granularity defined in the access control policy shall be commensurate with the level of risk of unauthorised access to its IT assets. 10.54 A financial institution shall adhere to the following principles: (a) adopt a “deny all” access control policy for users by default because all access to IT assets must be explicitly authorised; (b) employ “least privilege” access rights to ensure IT assets are accessed on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; (c) employ time-bound access which restrict access to a specific period based on the	Customers should employ appropriate identity authentication and access control mechanisms to manage access to information assets, establish a user access matrix, and conduct regular reviews and updates of the matrix. Customers should also formulate effective password rules and implement multi-factor authentication for accounts on critical systems. Additionally, customers should log all access records and user management activities for all users, facilitating audits and investigations. Customers can use Cloud Access Management (CAM) to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. CAM also supports viewing and tracking employee operation records through CloudAudit. Cloud Audit records all operation logs for Tencent Cloud accounts via APIs or the Tencent Cloud console for the most recent 90 days. Using the trail set feature, customers can persistently store all activity information from their accounts to COS. 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 supports configuring user access time, ensuring that access permissions are restricted to specific

No.	Domain	Summary of Controls	Tencent Cloud's Response
		nature of work;	time periods. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents.
		(d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features.	To support regulatory compliance, Tencent Cloud has also established internal access control authorization policies and a role-separation matrix. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud uses a zero-trust security management system to authenticate employee access, requiring users to complete two-factor authentication through the system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions to employees only based on job responsibilities and business necessities. Regular permission reviews are conducted to prevent permission misuse and abuse.
		(e) establish criteria for activities that require dual authorization control; and	
		(f) adopt robust user authorization and authentication based on criticality of IT assets.	
		10.55 A financial institution must employ multi-factor authentication (MFA) that can defend against social engineering attacks for authenticating user access, to critical systems. The MFA must combine two or more of knowledge factors, inherent factors.	Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. If customers encounter any issues related to accounts, network security, or product usage, they can submit a support ticket through the console to obtain technical assistance. Tencent Cloud provides a comprehensive operational security framework to ensure that service teams cannot directly access customer information assets without explicit customer consent and authorization.
		10.56 A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.	Tencent Cloud implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the IT security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. The production environment is fully equipped with bastion hosts, which centrally
		10.57 A financial institution must ensure—	
		(a) access controls to enterprise-wide systems are effectively managed and monitored;	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(b) anomalies are flagged for prompt investigations to contain any cyber incidents; and	manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
		(c) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	

9.2 Cybersecurity Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
11.6 11.7	Cyber Risk Management	11.6 A financial institution must conduct a realistic "Red Team" simulation attack on its infrastructure at least once every three years to proactively identify and manage potential vulnerabilities. 11.7 A financial institution may implement crowdsourced security testing programs as a complement to existing security assessments, in order to thoroughly test the security of their IT environment. The financial institution must engage reputable and credible service providers to facilitate the program.	Customers should conduct a comprehensive red team simulation attack on the infrastructure at least once every three years and implement crowdsourced security testing programs to comprehensively test and identify potential vulnerabilities in the managed IT environment. For penetration testing, Tencent Cloud offers the Penetration Testing Service (PTS), which fully simulates attack techniques and vulnerability exploitation methods commonly used by hackers. PTS uses controlled, non-destructive approaches to deeply probe the security of target systems, identify weaknesses in targets and network devices, and provide hardening recommendations to help customers improve system security. It also supports validation after vulnerability remediation. For vulnerability scanning, customers can use the Vulnerability Scanning Service (VSS) to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security

No.	Domain	Summary of Controls	Tencent Cloud's Response
			scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation advice to reduce security risks. To support regulatory compliance, Tencent Cloud regularly schedules vulnerability scans for cloud environment assets and analyzes, categorizes, and remediates detected vulnerabilities. Tencent Cloud also conducts full-chain large-scale penetration tests to proactively identify and fix potential security risks and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated via security tickets to responsible departments for timely remediation or compensating controls. Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.
11.9-11.11	Cybersecurity Operations	11.9 A financial institution must ensure continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure to prevent potential compromise of its security controls or weakening of its security posture. This shall include: (a) establishing a Security Operations Center (SOC) supported by competent resources and equipped with the necessary tools and	Customers should establish a security operation center to conduct continuous and proactive monitoring and detection of abnormal activities in the technical infrastructure and take appropriate responses. Additionally, customers should establish mechanisms for collecting, analyzing, and evaluating network threat intelligence, and promptly detect network threats. The Cloud Security Center (CSC) aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technologies for proactive monitoring of its technology security posture;	cloud log auditing and forensic analysis. Customers can also use Cloud Audit to record logs and continuously monitor account activity across Tencent Cloud infrastructure.
		(b) ensuring the scope of monitoring must cover all critical systems including the supporting infrastructure; and	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.
		(c) conducting regular review of its security posture via the conduct of a vulnerability assessment and penetration testing.	
		11.10 Financial institutions must establish a process to collect, analyse and evaluate cyber threat information in relation to the financial institution's environment ("cyber threat intelligence") to promptly detect cyber threats, including data breach incidents and spread of misleading information in relation to the financial institution over the Internet.	Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable.
		11.11 A financial institution must establish appropriate response to investigate and respond to flagged anomalous activities based on their level of complexity.	Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Tencent Cloud also operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			servers, and uses a ticketing system to track and resolve identified security issues. Tencent Cloud has defined detailed operational security “red lines” and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts.
11.12-11.16	Cyber Response and Recovery	11.12 A financial institution must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident. 11.13 A financial institution must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP must address the following: (a) Preparedness: Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident. (b) Detection and analysis:	Customers should establish comprehensive cyber crisis management policies and procedures, formulate a cyber incident response plan and define the roles and responsibilities of the cyber emergency response team, ensuring that the team members are familiar with the incident response plan and the handling procedures. Additionally, customers should establish an internal and external communication plan to ensure continuous coordination and communication with stakeholders during the crisis. Customers should also conduct at least one cyber drill exercise per year to test the effectiveness of the cyber incident response plan. For incident response and management, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. During the process of receiving, investigating, evaluating, handling and tracking information security incidents, the relevant responsible departments will maintain the relevant records of the received information security incidents and ensure the completeness and confidentiality of the records. For major security incidents,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Ensure effective and expedient processes for identifying points of compromise, assessing the extent of damage and preserving sufficient evidence for forensics purposes. (c) Containment, and eradication: Identify and implement remedial actions to prevent or minimise damage to the financial institution, contain and remove the known threats and resume business activities. (d) Recovery: Implement multiple strategies including contingency plans as part of incident recovery to swiftly resume business operations and significantly enhance redundancy and resilience. (e) Post-incident activity: Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations. 11.14 A financial institution must ensure that relevant CERT members are conversant with the incident response plan and handling procedures and remain contactable at all times. 11.15 A financial institution shall establish a secure and reliable out-of-band communication method for both internal and external stakeholders to ensure continued coordination and communication if the primary channel is rendered	Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type, frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence. In terms of communication and notification of the incident, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses. Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		unavailable during a crisis. 11.16 A financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP including the out-of band communication methods, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. The result of the annual cyber drill exercise must be reported to the Board in a timely manner. The out-of-band communication methods must also be tested regularly as part of the institutions cyber drill exercises. The test scenarios must include scenarios designed to test: (a) the effectiveness of escalation, internal and external communication and decision-making processes that correspond to different impact levels of a cyber-incident; and (b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.	operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services. In terms of cyber drill exercise, Tencent Cloud has established a cybersecurity contingency plan covering multiple cybersecurity emergency scenarios such as network attacks, malicious programs, data security incidents, equipment and facility failures, and catastrophic events. Built on a sound contingency plan system and supported by a dedicated emergency response team, the plan prioritizes the standardization of emergency response processes, further enhances capabilities in monitoring and early warning, and notification and disposal, and prevents and mitigates the adverse impacts of cybersecurity incidents on Tencent Cloud. In addition, relevant internal business departments of Tencent Cloud conduct regular training and drills on security incident contingency plans. They also provide technical training to security team members in accordance with the latest developments and trends in security technologies, ensuring that employees understand and comply with the latest security regulations and operational procedures, master up-to-date information security standards and best practices, and are able to respond quickly and effectively when security incidents occur.

9.3 Technology Audits

No.	Domain	Summary of Controls	Tencent Cloud's Response
13.1-13.4	Audit function	13.1 A financial institution must ensure that the scope, frequency, and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.	Customers should establish an IT audit mechanism, conduct regular technology risk audits, and ensure that IT auditors possess the necessary professional competence and skills.
		13.2 A financial institution must establish annual review on its technology audit plan that provides appropriate frequency and coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services.	Tencent Cloud will cooperate with the Customer's third-party security audits and supervision in accordance with applicable agreements and provide dedicated assistance to actively support Customer-initiated audit activities. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards.
		13.3 A financial institution must ensure the internal audit function must have dedicated technology audit resources with specialized competencies and professionally certified. The technology audit resources shall be adequately conversant with the developing sophisticate of the financial institution's technology systems, delivery channels and have sound knowledge in the areas audited.	Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center .
		13.4 The technology audit resources may be enlisted to provide advice on compliance and adequacy of control processes during the planning and development phases of	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		new major products, systems, adoption of third party service providers or technology operations. In such cases, the technology auditors participating in this capacity are expected to carefully consider whether such an advisory or consulting role can materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.	

9.4 External Party Assurance

No.	Domain	Summary of Controls	Tencent Cloud's Response
14.1 、 14.2	External Party Assurance	14.1 A financial institution shall appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA). The assessment must consider all major risks and determine the current level of resilience of the production data centre. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.24 to 10.28 have been adhered to. For data centres managed by third party service providers, a financial institution shall only rely on independent third party assurance reports provided such reliance is consistent with	Customers should appoint a technically competent external service provider to carry out regular network resilience and risk assessments. For data centers managed by a third party, customers can rely on the results of the third-party assessment reports. As a cloud service provider, Tencent Cloud is committed to delivering secure, stable, continuous, and reliable physical infrastructure for customers. In 2026, Tencent Cloud launched three data centers in Malaysia. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.	annual on-site audits to verify that data center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures.
		14.2 A financial institution shall appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the financial institution's adherence to the requirements in paragraphs 10.36 to 10.43. The designated board-level committee must deliberate the outcome of the assessment.	Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center .

9.5 Security Awareness and Training

No.	Domain	Summary of Controls	Tencent Cloud's Response
15.1-15.3	Internal Awareness and Training	15.1 A financial institution must provide adequate and regular technology and cybersecurity awareness	Customers should formulate a cybersecurity training plan and conduct regular training on technology and cybersecurity awareness for all employees and third-party service providers.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		education for all staff in undertaking their respective roles and measure the effectiveness of its education and awareness programs. This cybersecurity awareness education must be conducted at least annually and must reflect the evolving cyber threat landscape and emerging risks.	Additionally, customers should provide specialized training for personnel involved in technical operations, cybersecurity, and risk management, as well as board members, to ensure they can effectively perform their duties.
		15.2 A financial institution must provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent and suitably certified to effectively perform their roles and responsibilities.	To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Framework, which requires all formal employees, consultants, interns, and outsourced staff to complete information security training courses. These courses include mandatory training for all staff, specialized training for key roles, and optional professional courses. The training content covers areas such as basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.
		15.3 A financial institution must provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.	Tencent Cloud provides customers with Tencent Cloud Training and Certification based on Tencent Cloud product expertise and related professional capabilities. Through its official website, Tencent Cloud also offers operational procedures, user manuals, and other resources for cloud products to enhance customers' technical abilities and cloud proficiency.

9.6 Consultation and Notification related to Cloud Services and Emerging Technology

No.	Domain	Summary of Controls	Tencent Cloud's Response
17.1	Consultation and Notification related to Cloud Services and Emerging Technology	17.1 A financial institution is required to consult the Bank prior to the first-time adoption of public cloud or emerging technology for critical systems. During the consultation, the financial institution must demonstrate that specific risks associated with the use of these	If a customer adopts public cloud for their critical system for the first time, they should consult with the Bank and conduct a comprehensive risk assessment of the proposed cloud services, and also conduct a third-party review of the public cloud before implementation. Tencent Cloud undergoes annual professional

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technologies have been adequately considered and addressed to the satisfaction of the Bank, in order to proceed with the adoption of the public cloud for critical systems for the first time. The financial institution shall undertake the following prior to consulting the Bank on its adoption of public cloud for critical systems: (a) conduct a comprehensive risk assessment of the proposed cloud adoption or emerging technology, including the possible impact and measures to address and mitigate the identified risks. For public cloud, the assessment must follow the risk outlined in paragraph 10.50 and Appendix 10. (b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee the financial institution's readiness to adopt public cloud for critical system. (c) perform a third party pre-implementation review on public cloud or emerging technology. This review shall encompass the areas set out in Appendix 10 (for public cloud).	audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center. Tencent Cloud will, as appropriate, assign dedicated personnel to actively respond to and support audit and supervisory requirements from customers. For more detailed information about cloud services, please refer to Section 9.8 "9.8 Key Risks and Control Measures for Cloud Services".

9.7 Control Measures on Cybersecurity

No.	Domain	Summary of Controls	Tencent Cloud's Response
A	Network Security	1. A financial institution must ensure technology networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including but not limited to firewall and Intrusion Prevention System (IPS). This must include network for delivery of digital services and wireless networks as well. 2. A financial institution must ensure security controls for server-to-server external network connections include the following: (a) use PKI-based authentication method or equivalent alternatives; (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus. 3. A financial institution must ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter	Customers should implement necessary cybersecurity control measures, such as segmenting and zoning the technical network based on threat characteristics, deploying cyber security devices, protecting external network connections with secure tunnels, controlling remote access to servers securely, preventing tampering through clock synchronization, and subscribing to or purchasing solutions that can resist DDoS attacks, etc. For network segmentation or partitioning, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. For secure network communication, customer interactions on the Tencent Cloud console are encrypted using HTTPS. VPN Connection enables secure transmission between on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet Key Exchange) and IPsec protocols to encrypt data, creating a secure and trusted channel over the Internet. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		defences and protection such as firewall, IPS and antivirus; (d) close relevant ports immediately upon expiry of remote access; and (e) implement multi-factor authentication (MFA) for all remote access sessions. 4. A financial institution must ensure overall security controls are implemented including the following: (a) dedicated firewalls at all critical segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and “fail-close” mode activated; (b) IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic; (c) web and email filtering systems such as web-application firewalls, web-proxy, URL filtering, sandboxing features, spam filter and anti-spoofing controls; (d) end-point protection solution to detect and remove security threats such as malware; (e) enforce full hard disk encryption for all endpoints and systems; (f) solution to mitigate advanced persistent threats including zero-day and	Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services. <u>Cloud Firewall (CFW)</u> provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. <u>Web Application Firewall (WAF)</u> helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. For remote access, to enable customers to securely and quickly access cloud business systems anytime, anywhere, and from any mainstream device, Tencent Cloud supports SSL VPN technology for remote access. SSL VPN encrypts data transmitted over the Internet to ensure security and provides access control mechanisms to reduce unauthorized access. Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect through encrypted communication channels to access Tencent Cloud's corporate network and office systems remotely. Tencent Cloud maintains remote access logs to record user activities. Furthermore, Tencent Cloud's internal office network is completely isolated from the production environment where Customer data resides. When Tencent Cloud employees obtain customer consent and authorization to access customer information assets, they must access the production environment where customer data resides through a bastion host with two-factor authentication. In terms of host terminal protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to provide comprehensive monitoring and control of all server endpoint

No.	Domain	Summary of Controls	Tencent Cloud's Response
		signatureless malware; and	assets. The EDR solution supports antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing of command operations and login activities. It triggers alerts upon detecting malicious programs or abnormal behaviors, and Tencent Cloud follows up and handles these alerts through its ticketing system.
		(g) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.	
		5. A financial institution must synchronise and protect the Network Time Protocol (NTP) server against tampering.	For clock synchronization , Tencent Cloud displays the current accurate Universal Coordinated Time (UTC) through the Network Time Protocol (NTP). Tencent Cloud provides an internal NTP server for Tencent Cloud instances to use. For non-Tencent Cloud devices, customers can use the public NTP server provided by Tencent Cloud. Tencent Cloud regularly checks the time synchronization status of NTP servers to ensure unified, accurate, and reliable time across the entire network.
		6. A financial institution must ensure its technology systems and infrastructure, including critical systems outsourced to or hosted by third party service providers, are adequately protected against all types of Distributed Denial of Service (DDoS) attacks (including Domain Name Service (DNS) based, volumetric, protocol and application layer attacks) through the following measures:	To assist customers in preventing DDoS attacks , 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.
		(a) subscribing to DDoS mitigation services, which include automatic 'clean pipe' services to filter and divert any potential malicious traffic away from the network bandwidth; and	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.
		(b) regularly assessing the capability of the provider to expand network bandwidth on-demand including upstream provider capability, adequacy of the provider's incident response plan and its responsiveness to an attack;	
		(c) implementing geolocation	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		controls based on customer profile location, trend or behaviours, in order to restrict access from unauthorised regions and reduce exposure to malicious traffic.	
B	Data Security	1. A financial institution shall ensure that all data-at-rest of personal identifiable information (PII) and transaction data are securely protected and rendered unreadable to unauthorized access through the implementation of robust encryption mechanisms or equivalent capabilities. 2. A financial institution must design internal control procedures and implement appropriate technology in all applications and access points to enforce Data Loss Provision (DLP) policies and trigger any policy violations. The technology deployed must cover the following: (a) data in-use – data being processed by IT resources; (b) data in-motion – data being transmitted on the network; (c) data at-rest – data stored in storage mediums such as servers, backup media and databases. 3. A financial institution must implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to	Customers should adopt encryption measures to protect all data-at-rest of personal identifiable information (PII) and transaction data and implement necessary strategies for data prevention leakage. Additionally, customers should formulate and implement data removal strategies for devices or storage media and conduct continuous review and prevention of incidents of customer information breach. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access Customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with applicable laws and regulations during investigations by national or local authorities. For data storage protection, Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption keys are managed through the integrated Key Management Service (KMS), which provides full lifecycle management. Key Management Service (KMS) uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect keys and supports key rotation to reduce the risk of compromise or misuse. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance

No.	Domain	Summary of Controls	Tencent Cloud's Response
		prevent unauthorised access to data.	data transmission security using the following services:
		4. A financial institution must establish a clear DLP strategy and processes in order to ensure that proprietary and customer and counterparty information is identified, classified and secured. At a minimum, a financial institution must —	• <u>Direct Connect (DC)</u>: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • <u>VPN Connection</u>: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission.
		(a) ensure that data owners are accountable and responsible for identifying and appropriately classifying data;	Tencent Cloud provides secure and reliable data destruction mechanisms. When a customer's service is terminated, Tencent Cloud follows strict data erasure procedures to completely remove Customer data before reusing any previously purchased compute or storage resources. If media used to deliver Tencent Cloud services fails and requires replacement or reaches end-of-life, Tencent Cloud promptly performs thorough physical destruction in accordance with strict processes. In terms of data ownership and restrictions on third-party data access, Tencent Cloud provides <u>Data Security Audit (DSA)</u>, 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.
		(b) undertake a data discovery process prior to the development of a data classification scheme and data inventory; and	
		(c) ensure that data accessible by third parties is clearly identified and policies must be implemented to safeguard and control third party access. This includes adequate contractual agreements to protect the interests of the financial institution and its customers.	
		5. A financial institution must ensure adequate security controls are in place to safeguard against customer information breach (CIB), which include:	Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities.
		(a) conducting continuous review to ensure that CIB does not occur in the IT environments of the financial institution, its intermediaries,	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		or third party service providers. The financial institutions shall also incorporate scanning or screening of customer information into the scope of periodic security assessments (e.g., penetration testing, red teaming, or other security validation exercises); (b) enhancing cybersecurity operations to promptly detect and strengthen the safeguards against CIB; (c) ensure that the scope of financial institutions' internal audit reviews encompasses the management and security controls pertaining to CIB; and (d) conduct a thorough investigation to identify the technical root cause(s) of all CIBs with appropriate action and consequence management to mitigate recurrence.	Additionally, Tencent Cloud deploys DLP tools on employee computers to restrict external data export and monitor, detect, and prevent potential data exfiltration attempts. Regarding incident communication and notification, in the event of a customer data breach, Tencent Cloud will record and track the security incident through its internal security operations system, and notify affected customers in a timely manner as stipulated in the contract and required by regulations. The responsible departments will, upon completion of the incident remediation and handling, analyze the cause, type, losses, and responsibilities of the incident, compile an investigation and handling report on the information security incident, and collaborate with customers to complete the incident handling and reporting process.
C	Security Operations Centre (SOC)	1. A financial institution must ensure its SOC, has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the financial institution to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the financial institution's reviews of its cybersecurity posture and	Customers should establish a security operation center to conduct continuous and proactive monitoring and detection of abnormal activities in the technical infrastructure and take appropriate responses. Additionally, customers should establish mechanisms for collecting, analyzing, and evaluating network threat intelligence, and promptly detect network threats. Customers may use Cloud Log Service (CLS), a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. The Cloud Security Center (CSC) aggregates security-related data across Tencent Cloud, including

No.	Domain	Summary of Controls	Tencent Cloud's Response
		strategy.	alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Customers can also use Cloud Audit to record logs and continuously monitor account activity across Tencent Cloud infrastructure. Elasticsearch Service (ES) enables customers to stream real-time logs from cloud servers, containers, and other cloud products, as well as ingest historical and incremental business data into Tencent Cloud ES clusters for distributed storage and analytical queries.
		2. The SOC must be able to perform the following functions:	
		(a) adequate log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);	
		(b) incident coordination and response;	
		(c) vulnerability management;	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.
		(d) threat hunting;	
		(e) remediation functions including the ability to perform forensic artifact handling, malware and implant analysis;	
		(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations and monitoring Indicators of Compromise (IoCs). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers;	Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and
		(g) has a well-documented and standardized playbook that covers common and plausible cyber threat scenarios, such as ransomware attacks.	
		3. A financial institution must ensure that the SOC provides	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		monthly threat assessment report, which shall include, at a minimum, the following: (a) trends and statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centres and criticality of applications; and (b) intelligence on emerging and potential threats including Tactics, Techniques and Procedures (TTP). 4. A financial institution must subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures. 5. A financial institution must ensure the following: (a) the SOC is located in a physically secure environment with proper access controls; (b) the SOC operates on a 24x7 basis with disaster recovery capability to ensure continuous availability; and (c) the SOC has a holistic and end-to-end view of the financial institution's infrastructure including internal and external facing perimeters.	actionable. Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Tencent Cloud also operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls, and servers, and uses a ticketing system to track and resolve identified security issues. Tencent Cloud has defined detailed operational security "red lines" and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts.
D	Vulnerability Assessment and Penetration	1. A financial institution must establish standard operating procedures (SOP) for VAPT activities to continuously	Customers should regularly conduct vulnerability assessments and penetration tests to identify security weaknesses and evaluate

No.	Domain	Summary of Controls	Tencent Cloud's Response
	Test (VAPT)	identify vulnerabilities, assess potential risks and remediate the identified gaps. The SOP must outline the relevant control measures including but not limited to ensuring that the activities of external penetration testers are within the defined scope and are always subject to continuous oversight, validating the event logs and ensuring data purging. 2. A financial institution must perform a quarterly vulnerability assessment of external and internal network components that support all critical systems. 3. A financial institution must conduct annual intelligence-led penetration tests on its internal and external network infrastructure, critical systems as well as digital services including web, mobile and all external-facing applications. The test shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A financial institution must engage suitably accredited penetration testers and service providers to perform this function. 4. In addition to the periodic testing, a financial institution must also conduct intelligence-led penetration tests prior to introducing new systems for the new products or services to ensure the IT infrastructure is	their cybersecurity defense capabilities. For penetration testing, Tencent Cloud offers the Penetration Testing Service (PTS), which fully simulates attack techniques and vulnerability exploitation methods commonly used by hackers. PTS uses controlled, non-destructive approaches to deeply probe the security of target systems, identify weaknesses in targets and network devices, and provide hardening recommendations to help customers improve system security. It also supports validation after vulnerability remediation. For vulnerability scanning, customers can use the Vulnerability Scanning Service (VSS) to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation advice to reduce security risks. VSS can integrate with other Tencent Cloud products such as Host Security and Web Application Firewall to achieve a closed-loop process from risk monitoring to risk mitigation. To support regulatory compliance, Tencent Cloud regularly schedules vulnerability scans for cloud environment assets and analyzes, categorizes, and remediates detected vulnerabilities. Tencent Cloud also conducts full-chain large-scale penetration tests to proactively identify and fix potential security risks and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated via security tickets to responsible departments for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		not accidentally exposed due to unchecked network configuration.	timely remediation or compensating controls.
		5. A financial institution must ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions.	Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.
		6. A financial institution must undertake an independent compromise assessment on the technology infrastructure of its critical systems at least once every three years and ensure the results of such assessments are escalated to senior management and the board in a timely manner. The financial institution may leverage their group-level cyber risk management functions to support this requirement.	
E	Application Programming Interface (API) Security	1. A financial institution must ensure that the level of API security implemented is commensurate with the potential risks involved. At a minimum, financial institutions are required to implement the following measures to mitigate cybersecurity risks associated with APIs: (a) implement and maintain a centralized API inventory. The inventory must comprehensively encompass	Customers should adopt encryption standards and key management controls to ensure the security of sensitive data transmitted through the API, and implement fine-grained access control and the principle of least privilege to protect the API, and also implement robust identity and access management to verify service requests. Customers should establish detection mechanisms to visualize the usage and performance of the API, promptly detect suspicious activities, and implement necessary measures to defend against cybersecurity attacks. TencentCloud API support HTTPS transmission encryption and implement multiple

No.	Domain	Summary of Controls	Tencent Cloud's Response
		identification, classification and prioritisation of all associated API connections and dependencies; (b) ensure availability of API service by designing APIs to be scalable for handling high level of traffic and implementing measures to mitigate denial of service attacks; (c) undertake secure coding practices during API development, which shall include but not be limited to validating security of third party code and libraries, implementing robust error handling, input validation and appropriate security headers; (d) employ robust encryption standards and effective key management controls; (e) deploy anti brute-force mechanisms such as rate limiting, account lockout, captcha challenges, and others; (f) implement strong and robust authorisation and authentication protocols that commensurate with the risks presented by the APIs; (g) consider utilizing an API gateway to manage access, authentication, and authorization of the APIs; (h) conduct periodic security assessments on APIs, including penetration testing and static / dynamic security testing; (i) continuous monitoring for	SDK-based signature mechanisms (such as PHP, Python, Java, .NET, Node.js) for API authentication. Additionally, Tencent Cloud uses Timestamp-based signature expiration to prevent replay attacks. Signature encryption supports HmacSHA1 and the more secure HmacSHA256, ensuring the integrity and security of API requests and providing port-level communication security for customers' business operations. 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: • <u>Web Application Firewall (WAF):</u> 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. • <u>TencentCloud API</u> 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. • <u>CloudAudit:</u> 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		APIs to ensure visibility into the utilization and performance of the APIs, for prompt identification and detection of potential suspicious activities; and (j) establish process to effectively revoke access token or API keys in the event of a compromise.	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.

9.8 Key Risks and Control Measures for Cloud Services

9.8.1 Cloud Governance

No.	Domain	Summary of Controls	Tencent Cloud's Response
3	Due diligence	Due diligence on the prospective cloud service providers should be risk-based and conducted to a level of scrutiny that is commensurate with the criticality of the information and technology assets to be hosted on the cloud in compliance with relevant requirements and guidance as stipulated in the Third Party Service Provider Management section of this policy document and paragraphs 9, 10 and 11 in the Bank's Outsourcing policy document (Outsourcing process and management of risks, Outsourcing outside Malaysia, Outsourcing involving cloud services).	Customers should conduct due diligence before the third-party service provider is hired, as well as throughout the entire service period. 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. For more details on due diligence, please refer to Section 5 "How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing" clause "9.2, 9.3 Assessment of service provider".
4	Access to cloud service providers' certifications	A financial institution should review their cloud service providers' certifications prior to entering into any cloud arrangement or contract with	Before signing a cloud service agreement or contract with a service provider, customers should review the provider's certifications to ensure that the cloud service provider complies with relevant laws and regulations and provides

No.	Domain	Summary of Controls	Tencent Cloud's Response
		such cloud service providers. At a minimum, a financial institution should: (a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider's action plans for mitigating any noncompliance; and (b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. The financial institution's risk assessment should address all the requirements and guidance as stipulated in the Cloud Services section of this policy document and the Bank's policy document on Outsourcing which sets out provisions on outsourcing involving cloud services.	reports on the cloud platform issued by a reliable independent external institution. Tencent Cloud has obtained several security and privacy compliance certifications and qualifications, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. These certifications demonstrate that Tencent Cloud's security management and personal data protection practices meet relevant certification standards or industry's best practices. For more detailed information about the authoritative certifications obtained by Tencent Cloud and the completed third-party independent evaluations/audits, please refer to Section 2 "Tencent Cloud Security and Privacy Compliance".
5	Contract management	A financial institution should set out clearly and where relevant, measurable, contractually agreed terms and parameters on the information security and operational standards expected of the cloud service providers. Such contract terms and parameters should be aligned with the financial institution's business strategy, information security policies and regulatory	Customers should sign a contract with the cloud service provider that covers the terms and parameters regarding information security and operational standards. They should also pay attention to the risks associated with the service provider, such as cross-border risks, data retention and access risks, as well as subcontractor risks, etc. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		requirements. (a) The terms of the contracts between the financial institution and cloud service providers should address the risks associated with cloud services and third party service providers; (b) Jurisdiction risk may arise because cloud service providers operate regionally or globally in nature and may be subject to the laws and regulatory requirements of its home country, the location of incorporation, and the country where the client receives the service. (c) A financial institution should assess the potential impact and formalise arrangements with cloud service providers to comply with local laws and regulatory requirements for incident investigation and law enforcement purposes. This would include adhering to data retention requirements and data access procedural arrangements to ensure the confidentiality and privacy of the customers are protected; and (d) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth party service providers (such as sub-contractors), which could	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 Bank and financial institutions. Tencent Cloud strictly complies with the laws and regulations of the jurisdictions in which it operates to protect user privacy and data security. Tencent Cloud actively cooperates with customers' outsourcing-management requirements and responds to and participates in audits or assessments initiated by customers.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		change rapidly. For example, customer data could be leaked due to exposure caused by fourth party service providers.	
6	Oversight over cloud service providers	A financial institution should ensure effective oversight over cloud service providers taking into account the fact that the cloud service providers may engage subcontractor(s) to provide cloud services. This includes, at a minimum, the following: (a) establish and define a continuous monitoring mechanism with alignment to the enterprise outsourcing risk management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis; (b) identify, assign and document the key responsibilities within the financial institution for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined; (c) perform assessments of the outsourcing arrangement involving cloud service providers periodically in accordance with the financial institution's internal policy to achieve business resilience	Customers should effectively monitor the cloud service provider and its subcontractors to ensure compliance with the agreed service level agreements and relevant laws and regulations. Customers should also regularly assess the outsourcing arrangements involving the cloud service provider and conduct timely reviews and evaluations when significant changes occur in the cloud risk situation. 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 support customers' outsourcing oversight requirements, Tencent Cloud will, in accordance with actual circumstances and contractual agreements, cooperate with third-party audits and provide dedicated assistance, actively responding to customer-initiated audit activities. Additionally, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture and ensure compliance with applicable laws, regulations, and security management standards. Tencent Cloud also undergoes regular independent third-party professional audits and provides assurance reports on system and organizational controls to cloud customers, independent auditors, regulators, shareholders, and other stakeholders,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		with emphasis on data security and ensure prompt notification to the Bank of the developments that may result in material impact to the financial institution (such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development) in line with the Bank's policy document on Outsourcing (Outsourcing PD), in particular, provisions relating to outsourcing of cloud services outside Malaysia; (d) promptly review or re-perform risk assessment upon any material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development.	disclosing the latest internal control status of Tencent Cloud services. For security incidents that may impact customers, Tencent Cloud, after internal review based on the scope and severity of the information security incident, notifies customers of the incident handling and analysis results through appropriate means and provides corresponding technical support. This assists customers in taking remedial measures to minimize losses.
7	Skilled personnel with knowledge on cloud services	(a) The adoption of cloud services requires commensurate changes to the financial institution's internal resources and process capabilities. In this regard, a financial institution should: i) equip its board and senior management with appropriate knowledge to conduct effective oversight over the cloud adoption; and ii) ensure its IT and security operations or relevant personnel are appropriately skilled in the areas of cloud design, migration, security	Customers should ensure that the personnel involved in cloud services, including management, IT and security operations, finance, law, risk compliance, internal audit and other departments, possess the appropriate knowledge and relevant professional skills. Moreover, adequate training should be provided to the employees to ensure they understand their own responsibilities regarding cloud usage. Tencent Cloud provides customers with Tencent Cloud Training and Certification based on Tencent Cloud product expertise and related professional capabilities. Through its official website, Tencent Cloud also offers operational procedures, user manuals, and other resources for cloud products to enhance customers' technical abilities and cloud proficiency.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		configurations, including administrative, monitoring and incident response; (b) The effective management of cloud services is not purely the responsibility of the financial institutions' IT function. Therefore, a financial institution should ensure relevant internal resources in business operations, finance, procurement, legal, risk and compliance are also adequately skilled and engaged to manage the change in risk profile arising from cloud adoption. This should also enable financial institutions to respond effectively to operational incidents; (c) A financial institution should equip internal audit and personnel undertaking the risk management and compliance functions with relevant cloud computing and cloud security skills to be able to verify the effectiveness of the information security controls in alignment with the financial institution's cloud usage policy and information security objectives; (d) A financial institution should ensure that its staff receive adequate training to understand their responsibilities in complying with internal cloud usage policies and are prepared to effectively respond to a range of security incident scenarios	Tencent has established a Security Technology Committee and specialized security teams across different functions and domains, supported by an experienced industry expert service team dedicated to delivering secure, reliable, professional, and compliant products and services. Tencent Cloud has established robust HR management standards and procedures to ensure appropriate recruitment and placement based on job requirements. Background checks, including verification of education and certifications, are conducted during recruitment. Tencent Cloud has established diverse career development paths, equipped employees with abundant and high-quality learning resources, and continuously optimized training courses and systems to support employees' personal growth and career development. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		developed on a risk-based approach; and (e) A financial institution should expand the scope of the formal consequence management process to govern the use of cloud services to ensure the cloud usage policy is effectively enforced given that cyber hygiene is critical to ensure the continued security of cloud service usage.	

9.8.2 Cloud Design and Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
1	Cloud architecture	(a) A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application. (b) A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an “assume breach” mindset, layering defense-in-depth through micro-segmentation, “deny-by-default”, “least privilege” access rights, and conducting deep inspection and continuous validation where applicable. (c) A financial institution should use the latest network architecture approach and appropriate network design	Customers should adopt the latest network architecture solution and appropriate network design concepts and schemes to design a stable cloud architecture. Customers should build a layered defense architecture based on the zero-trust principle, use secure encrypted communication channels, and implement appropriate network isolation. In addition, customers should also implement strict management for APIs, configure secure access control, and continuously monitor and track. Tencent Cloud operates data centers across multiple global regions, organized by 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 based on business continuity and data security requirements, ensuring disaster recovery capabilities. For network segmentation or partitioning, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		concept and solutions for managing and monitoring granular network security and centralized network provision in managing complexity of the cloud network environment. (d) A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. (e) For financial institutions leveraging on their financial group's cloud infrastructure, the financial institutions should consider an appropriate level of network segregation (e.g., logical tenant isolation in the shared environment of the cloud) to mitigate the risk of cyber-attacks from propagating cross-border or cross-entity and affecting the Malaysian financial institution's operations. (f) The increasing use of application programming interfaces (API) by financial institution to interconnect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanagement may amplify the impact of an information security incident. A financial institution should ensure its APIs are subject to rigorous	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 a variety of services to customers, such as EdgeOne (EO) platform, Cloud Firewall (CFW), Web Application Firewall (WAF), Anti-DDoS, etc. For more detailed information on network security, please refer to the content of Clause "10.36-10.43 Network Resilience" in Section 9.1 "9.1 Technology Operations Management". 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. For secure network communication, customer interactions on the Tencent Cloud console are encrypted using HTTPS. VPN Connection enables secure transmission between on-premises data centers and Tencent Cloud resources. VPN tunnels use IKE (Internet Key Exchange) and IPsec protocols to encrypt data, creating a secure and trusted channel over the Internet. For tenant isolation, Tencent Cloud enforces resource access control at the virtualization layer, private network isolation policies, web

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management and control mechanisms which include the following: i) APIs should be designed for service resilience to avoid the risk of single points of failure and configured securely with appropriate access controls;and ii) APIs should be tracked and monitored against cyber-attacks with adequate incident response measures and are de-commissioned on a timely basis when no longer in use.	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. For APIs security management, TencentCloud API support HTTPS transmission encryption and implement multiple SDK-based signature mechanisms for API authentication. Additionally, Tencent Cloud uses Timestamp-based signature expiration to prevent replay attacks. Signature encryption supports HmacSHA1 and the more secure HmacSHA256, ensuring the integrity and security of API requests and providing port-level communication security for customers' business operations. Tencent Cloud uses Access Key as the credential for API calls to cloud resources. For more detailed information on APIs security management, please refer to the content of Clause "E Application Programming Interface (API) Security" in Section 9.7 "9.7 Control Measures on Cybersecurity".
2	Cloud application delivery models	(a) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. Currently, DevOps and Continuous Integration / Continuous Development (CI/CD) are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A financial	Customers should consider using immutable workloads and ensure that the images are tested before deploying them to the production environment. If the public cloud workloads are configured using Infrastructure as Code (IaC) approach, customers should implement necessary control measures to reduce the risk of configuration errors and protect the IaC configuration files. Tencent Cloud's Cloud Native Build (CNB) provides a complete developer toolchain, including code hosting, high-performance CI/CD pipelines, AI code assistant, and artifact management. The AI code assistant, designed specifically for developers, supports multiple mainstream programming languages and offers features such as code completion, unit testing,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		institution should ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure. (b) A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services and financial institutions are, among others, encouraged to: i) adopt industry best practices such as infrastructure-as-code (IaC) to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner; ii) use immutable infrastructure practices for deployment of services to reduce the risk of failure by creating a new environment with the latest stable version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to immutable infrastructure to improve compliance review and combat evolving cyber-attacks. (c) Where relevant, a financial institution should implement appropriate controls on the IaC process to minimise the risk of misconfiguration and reduce the cyberattack surface. This includes the following measures that should be taken	code diagnostics, intelligent reviews, and smart Q&A for code issues—helping developers improve coding 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. Tencent Cloud has established a set of secure development standards for information systems and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the product secure development lifecycle. This approach addresses different stages including requirements, design, development, testing, delivery, and operations, embedding information security and privacy protection principles into every phase to ensure that cloud products receive adequate security controls and assessments throughout their lifecycle. Tencent Cloud incorporates its Software Development Lifecycle (SDLC) into the DevSecOps process to ensure rapid and continuous development, release, and deployment of cloud products. Tencent Cloud has also established access control authorization policies and a privilege separation matrix to enforce segregation of duties among personnel responsible for development, testing, and release activities. To help customers manage and secure IaC configurations, Tencent Cloud provides Tencent Infrastructure Automation for Terraform.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		by the financial institution: i) conduct vulnerabilities scanning as part of IaC automation steps and ensure issues are remediated prior to the provisioning of IT infrastructure; ii) ensure virtual machine images (VMI) or container images of IaC templates are trusted and digitally signed; and iii) implement appropriate access control to prevent unauthorized changes to IaC templates.	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. Customers can also use Tencent Cloud Container Security Service (TCSS) to protect container and image security. TCSS supports container asset management, image security scanning, runtime intrusion detection, and security baseline configuration management, helping customers build a comprehensive container security protection system and providing full lifecycle protection for containers—from image creation and storage to runtime.
3	Virtualization and containerization management	The guidance provided in this paragraph is applicable to financial institutions which use or plan to use PaaS and IaaS cloud service models only. (a) A financial institution should ensure virtualization services are configured in line with the prevailing guidance from the cloud service providers and industry best practices, commensurate with the evolution of cloud computing technologies. (b) A financial institution should ensure virtual machine	Customers should ensure that the virtualization services are configured in line with the prevailing guidance from the cloud service providers and industry's best practices. The virtual machines and container images should be hardened and continuously monitored. In terms of security configuration management, Tencent Cloud's Cloud Security Center (CSC) provides automated configuration risk assessment capabilities to help customers reduce security risks caused by misconfigurations and improve overall cloud security posture. Customers can also use Config Audit to perform centralized auditing and governance of cloud resources, continuously recording configuration details and changes across different regions under their account.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and container images are configured, hardened, and monitored appropriately. This includes the following: i) use stable images and keep images up to date; ii) store and use images from trusted repositories or registries; iii) scan images for vulnerabilities, remediate any vulnerabilities prior running in production; iv) enforce “least privilege” access; v) harden images based on industry best practices; and vi) stored images are subjected to security monitoring from unauthorised access and changes.	Based on Tencent Cloud best practices and compliance templates, Config automatically evaluates resource configurations for compliance, identifies non-compliant resources, and enables automated monitoring and management of cloud resources. 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. For container image management, Tencent Cloud Container Registry (TCR) offers secure, dedicated, high-performance container image hosting and distribution services. Customers can also use Tencent Cloud Container Security Service (TCSS) to protect container and image security. TCSS supports container asset management, image vulnerability scanning, runtime intrusion detection, and security baseline configuration management, delivering full lifecycle protection from image creation and storage to runtime. To strengthen security controls for virtual machines and virtualization services, Tencent Cloud has established internal virtualization security management standards, defining responsibilities for resource management, access control, and configuration management. Tencent Cloud employs technologies such as virtual machine isolation, resource control, patch management, vulnerability protection, and hypervisor hardening to build a comprehensive virtualization security defence system. To secure container environments, Tencent Cloud has established a multi-layered container

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security architecture. For north-south traffic (between container cloud and external networks), Tencent Cloud leverages traditional security capabilities such as Web Application Firewall (WAF), DDoS protection, web vulnerability scanning, and Intrusion Detection and Prevention Systems (IDPS). For east-west traffic (within the container cloud), Tencent Cloud applies container-native security mechanisms based on principles such as security by design, shift-left security, and zero trust, implementing layered protections across infrastructure, container platform, and application layers. To support customers in meeting regulatory requirements, Tencent Cloud has established internal cybersecurity configuration standards and security baseline standards to standardize security configurations for network devices, firewalls, host operating systems, databases, and application systems. Security policies and parameter settings for network devices such as routers, firewalls, and servers are regularly reviewed to ensure effectiveness.
4	Change management	(a) A financial institution should establish a process to systematically assess and take appropriate action to manage the impact of the releases by cloud service providers in relation to existing infrastructure, network, upstream and downstream systems to minimize the impact of any service disruption. (b) A financial institution should ensure its existing change management process is extended to cover cloud services where appropriate to promote effective and secure	Customers should assess the impact of the releases by cloud service providers in relation to existing infrastructure, network, upstream and downstream systems, and extend the existing change management to the cloud service to ensure that all production environments have synchronized critical changes with the supported cloud regions and availability zones. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also maintains an emergency change management process, under which emergency changes must

No.	Domain	Summary of Controls	Tencent Cloud's Response
		system development. The escalation process and approving authority should be clearly defined to ensure critical changes can be implemented and risk of service disruptions are mitigated promptly. (c) All critical changes deployed to the production environment should also be timely applied across environments such as disaster recovery site or supported cloud regions and availability zones where appropriate.	receive appropriate approval before execution. All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment. Tencent Cloud classifies change requests based on attributes such as importance, urgency, and scope of impact. For changes that may affect external environments—such as product, infrastructure, or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels.
5	Cloud backup and recovery	(a) As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; ii) conduct periodic reviews of the cloud service providers' restoration and recovery capabilities; and iii) conduct testing of recovery	Customers should establish a backup management mechanism to back up the data and conduct regular backup and recovery tests to meet the system criticality and recovery point objectives. Customers should also regularly operate business at the recovery site, backup site or alternative site. In addition, customers should assess the resilience requirements of the cloud service and identify corresponding control measures based on the system criticality to ensure the availability of the service. Tencent Cloud operates data centers across multiple global regions, organized by 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		strategy prior to deployment of the system.	zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures.
		(b) A financial institution should ensure backup and restoration procedures are periodically tested to validate recovery capabilities. The frequency of backup procedures should be commensurate with the criticality of the system and recovery point objective (RPO) of the system. Remedial actions should be taken promptly by the financial institution for unsuccessful backups.	Tencent Cloud ensures complete isolation between different regions, maximizing stability and fault tolerance. Each region is further divided into multiple isolated availability zones to reduce the impact of single-point failures and guarantee business continuity for customers. 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.
		(c) A financial institution should ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following:	Tencent Cloud has implemented a comprehensive business continuity and disaster recovery management system certified to ISO/IEC 22301.
		i) ensure the capability to restore a virtual machine and container at point-in-time as per the business recovery objectives; and	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.
		ii) make virtual machine and container images available in a way that would allow the financial institutions to replicate those images at alternate sites or recovery sites;	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.
		(d) A financial institution should assess the resilience requirements of the cloud services and identify	For more information related to business

No.	Domain	Summary of Controls	Tencent Cloud's Response
		appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. Financial institutions should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentration risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones; ii) achieve geographical redundancy by having data centres in different geographical regions; iii) adopt hybrid cloud (combination of on-premises and public cloud setup); iv) establish back-up cloud service providers and identify appropriate arrangement for porting of data and application to ensure timely service resumption; and v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks.	continuity, please refer to Section 8 "8 How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Business Continuity Management", and for more information on service availability, please refer to Clause "10.32-10.35 Service Availability" of Section 9.1 "9.1 Technology Operations Management".
6	Interoperability and Portability	Interoperability standards for cloud services continue to	Customers should assess the technical requirements for the interoperability and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems or alternate cloud service providers, financial institutions are encouraged to: (a) assess technical requirements for interoperability and portability prior to entering into an agreement or arrangement with the cloud service providers to avoid vendor lock-in; (b) maintain a list of third party service providers and tools that are needed to facilitate a smooth transition; (c) ensure usage of standardized network and communication protocols for ease of interoperability and portability with on-premise IT systems or alternate cloud platforms; (d) ensure the use of common electronic data formats, where applicable, to ease the movement of data between cloud service providers or to on-premises IT system; and (e) extend patch and EOL management to ensure technology solutions employed remain effective and protected against system	portability of the cloud service provider, adopt standardized network and communication protocols and common electronic data formats, maintain a list of third-party service providers and tools necessary for migration, and extend patch and EOL management to the cloud environment. 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. 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. Tencent Cloud has established patch and end-of-life management in cloud-native environments. Regarding patch management, Tencent Cloud regularly identifies the latest patches, conducts security testing, notifies business teams for installation, uses detection tools to scan installation status, and automatically alerts for devices that exceed the installation deadline. For end-of-life management, Tencent Cloud maintains a detailed inventory of hardware and facilities in its Configuration Management Database (CMDB), including each server's End-of-Support (EOS) date and version information. Tencent Cloud regularly retires and replaces servers, while software components (such as operating systems and database systems) are upgraded to appropriate versions before reaching end-of-support. For decommissioned

No.	Domain	Summary of Controls	Tencent Cloud's Response
		vulnerabilities.	hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction in official logs.
7	Exit strategy	(a) A financial institution should establish a robust cloud exit strategy as part of its cloud risk management framework to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers. (b) A financial institution's exit strategy should be supported by an appropriate and proportionate exit plan that establishes the operational arrangements to facilitate an orderly exit from an agreement or arrangement with cloud service provider, including the following: i) conduct impact assessment to determine potential costs, resources, and timing implications of transferring cloud services to an alternative cloud service providers or rely on the in-house arrangement at the financial institution; ii) identify appropriate methods to port data and applications to an alternative arrangement; iii) to obtain written confirmation or attestation from the cloud service providers or independent external service providers that all sensitive data has been securely deleted from the cloud service provider's	Customers should establish a cloud exit strategy to ensure that the cloud service provider can orderly terminate the cooperation and securely delete all sensitive data in response to incidents such as sudden failures of the cloud service provider or termination of the contract. If customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate cloud data and production environments at any time. According to the service agreement between Tencent Cloud and the customer, if the cloud service expires or is terminated, customers must complete data migration before the retention period ends for any data stored on cloud servers through Tencent Cloud services. Tencent Cloud supports customers in backing up and migrating data using common standard formats. Customers can use the same transmission methods and protocols as during onboarding or leverage network services such as Direct Connect (DC) and VPN Connection to ensure secure and reliable data transfer during offboarding. After cloud services are terminated, Tencent Cloud will follow strict data erasure procedures and permanently delete all customer data, including replicas and backups, after the retention period. Deleted data cannot be restored. For hardware destruction, Tencent Cloud employs secure physical destruction methods to ensure that hard drives are completely destroyed, with the process duly recorded in the destruction log.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		system upon completion of the exit process; and iv) conduct testing to validate the effectiveness of the exit plan, to obtain a reasonable degree of assurance of its effectiveness.	
8	Cryptographic key management	(a) A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. (b) A financial institution should ensure its policies and procedures on cryptography are extended to cover cloud services where relevant, to promote the adoption of strong cryptographic controls. (c) Where appropriate and feasible, financial institutions should retain ownership and control of the encryption keys (themselves or with an independent key custodian), independent from the cloud service provider, to minimize the risk of unauthorised access to the data hosted on the cloud. (d) As the usage of cloud adoption increases, managing many encryption keys used for protecting data has become more complex and may introduce new challenges for financial institutions. A financial institution should adopt a comprehensive and centralized approach to key	Customers should establish a cryptographic key management policy and consider using industry-recognized encryption algorithms to encrypt the data, and also implement a key life cycle management mechanism to retain ownership and control over the encryption keys. In terms of data storage protection, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength encryption algorithms. Integrated Key Management Service (KMS) ensures full lifecycle management of encryption keys, safeguarding data confidentiality. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations. To help customers protect the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS). KMS enables customers to easily create and manage keys, meeting multi-application and multi-business key management needs while complying with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, allowing customers to apply encryption effortlessly. KMS supports external key import, allowing customers to use their own key material for encrypting and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management including the use of centralised key management system that can handle generations, storage and distribution of keys in a secure and scalable manner.	decrypting sensitive data on Tencent Cloud's architecture, thereby implementing a Bring Your Own Key (BYOK) solution on Tencent Cloud. KMS is built on FIPS 140-2 certified Hardware Security Modules (HSMs) for key generation and protection, uses secure data transmission protocols, and employs a multi-data-center distributed cluster architecture with hot backups. Underlying HSM devices are deployed with dual-site cold backups to ensure high availability of the key management system. Regarding internal encryption key management, Tencent Cloud has established encryption and key management standards that govern the processes of key application, generation, storage, usage, transmission, rotation, and destruction to ensure the confidentiality, integrity, and availability of keys. For more details on key management, please refer to Clause "10.20-10.23 Cryptography" of Section 9.1 "9.1 Technology Operations Management".
9	Access Controls	(a) Cloud computing where remote access is supported by default. Financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: i) allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management plane; ii) implement "least privilege" and strong multi-factor authentication (MFA); iii) employ granular entitlement allocation for privileged users;	Customers should establish an identity authentication and access control mechanism for data and information technology systems to manage access to information assets, control the access rights of external personnel, conduct regular reviews and updates of permissions, and enhance the security management of privileged user accounts by using multi-factor authentication and monitoring mechanisms. In addition, customers should also establish a secure remote access management mechanism. Customers can use Cloud Access Management (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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		iv) conduct continuous monitoring of the activities performed by privileged users; and v) ensure secure communication protocols are in place for accessing the management plane. (b) A financial institution should extend its user access matrix to cover user access rights for both the financial institution and its cloud service providers where relevant for the ongoing access to cloud services. (c) A financial institution should ensure their tenant access controls to all hypervisor management functions or administrative consoles for systems hosting virtualized systems are effectively implemented in accordance with the requirements and guidance under the Access Control section of this policy document. These controls should mitigate the risk of any unauthorised access to the hypervisor management functions and virtual machine. (d) Point-to-point connections with cloud services may proliferate with the ease of cloud adoption, resulting in fragmentation of identity and access management and the risk of unsanctioned data being migrated to the cloud.	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 security incidents. In terms of user authorization, Tencent Cloud has established internal access control management standards requiring user accounts to use unique identifiers and enforcing password policies for employee accounts based on security baselines. Tencent Cloud uses a Zero Trust security management system to authenticate employee access; users must complete multi-factor authentication before accessing internal resources. Tencent Cloud also implements authorization policies and a privilege separation matrix, maintaining records of personnel identity information mapped to job roles and corresponding permission levels for each business system. Regular internal permission reviews are conducted to prevent misuse or abuse of access rights. Any unnecessary access rights are promptly revoked. For privileged account management, Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain approval before accessing bastion hosts, and authorized personnel must complete secondary identity verification to log in. All backend operation records are stored centrally on a logging platform and reviewed periodically by Tencent Cloud's internal audit team. For remote access management, Tencent Cloud employees may only use trusted devices registered with Tencent Cloud and must access Tencent Cloud's office network and daily systems through encrypted communication channels. Remote access logs are maintained

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Financial institutions are encouraged to:	and reviewed regularly.
		i) where appropriate and commensurate with the size and complexity of the cloud adoption, implement a federated approach for identity and access management to mitigate risks of identities in cloud services being disjointed from the internal identities, unauthorised access and to ease user access management; and	For more detailed information on access control, please refer to the Clause "10.23 - 10.27 Access Controls" in Section 6.1 " 6.1 Control Environment ".
		ii) consider additional attributes in context-aware decisions for identity and access management such as pattern of access to further mitigate the risks associated with remote access.	
10	Cybersecurity Operations	(a) A financial institution should ensure the governance and management of cybersecurity operations is extended to cover cloud services, with appropriate control measures to prevent, detect, and respond to cyber incidents in the cloud environment to maintain the overall security posture of the institution. (b) The interconnected cloud service supply chain could become a source of cyber risk. A financial institution should ensure integrated monitoring and full visibility of cloud services are established. This should include the following:	Customers should implement necessary security control measures at its network boundary to restrict unauthorized system communication. Customers should establish the ability to detect cybersecurity threats, collect, process and analyze abnormal activities that may affect the business and IT environment. In addition, customers should conduct vulnerability assessments and penetration tests regularly to identify security vulnerabilities and evaluate its cybersecurity protection capabilities. The Cloud Security Center (CSC) aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Empowered by Threat Intelligence Center

No.	Domain	Summary of Controls	Tencent Cloud's Response
		i) continuous monitoring of system communications between the cloud service provider, on-premise IT systems and other service providers to ensure the security perimeter is not breached; and ii) ensuring that third party service providers, including those providing ancillary functions, have adequate capabilities to monitor, detect and respond to anomalous activities, with timely communication to the financial institution of relevant cyber incidents. (c) A financial institution should understand the segregation of responsibility in security management, which varies across the cloud service models. A financial institution should manage the sources of vulnerabilities appropriately including by: i) proactively seeking assurance of their cloud service providers to conduct periodic VAPT on the cloud infrastructure to ensure tenant isolation and overall security posture remains healthy; and ii) understanding the cloud service provider's VAPT policy for the financial institution on cloud infrastructure for IaaS model given the varying degree of the financial institution's access to the cloud environment and	<u>(TIX)</u>, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable. Tencent Cloud embraces the openness and shared nature of cloud computing services, continuously enhancing platform security and collaborating with customers to build a robust security framework. Tencent Cloud is responsible for the security of data center infrastructure and the cloud platform. Considering that control responsibilities vary across service models (IaaS, PaaS, SaaS), Tencent Cloud has established a Shared Responsibility Model, detailed in Section 3 "Tencent Cloud Security Responsibility Sharing Model". Based on this model, Tencent Cloud works closely with customers to address security challenges collaboratively. Tencent Cloud has established a regular vulnerability scanning and penetration testing mechanism. Vulnerability scanning systems generate scheduled tasks to scan assets within the cloud environment, and any detected vulnerabilities are analysed, categorized, and remediated. Tencent Cloud's security team conducts large-scale end-to-end penetration tests periodically and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated through security tickets to the responsible departments, which promptly patch vulnerabilities or implement compensating controls to ensure that exploitable weaknesses identified during testing are properly addressed.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		establish a VAPT arrangement with cloud service providers upfront which commensurate with the complexity of the cloud environment.	Meanwhile, Tencent Cloud also offers Penetration Testing Service (PTS) and Vulnerability Scanning Service (VSS) to customers. For more detailed information on cybersecurity operations, please refer to Section 9.2 "9.2 Cybersecurity Management".
11	Distributed Denial of Service (DDoS)	(a) A financial institution should ensure that its DDoS mitigation service is commensurate with the size and complexity of the cloud adoption. (b) The risk of a SPOF may surface when a financial institution leverages solely on a cloud-based solution to mitigate DDoS attacks. As such, a financial institution is encouraged to engage alternative DDOS mitigation providers or establish circuit breakers to avoid service disruption when the main DDOS mitigation provider is disrupted.	Customers should adopt DDoS mitigation service to promptly detect and respond to DDoS attacks (which may directly or indirectly cause system disruptions) and encourage them to engage alternative DDOS mitigation providers or establish circuit breakers. 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. To support customers in meeting regulatory requirements and defending against DDoS attacks, Tencent Cloud has deployed firewalls, intrusion detection/prevention systems (IDS/IPS), and DDoS protection tools, and conducts regular DDoS defense drills.
12	Data Loss Prevention (DLP)	(a) A financial institution should protect the data hosted in cloud services as required under the Data Security of Appendix 5 of this policy document, including the expansion of the endpoint footprint if the financial institution allows its staff to use their own devices to access the sensitive data. (b) As it becomes increasingly easy to distribute digital content to customers via cloud	Customers should formulate a data loss prevention strategy to protect the data processed and stored in the cloud environment, preventing unauthorized or accidental leakage of the data. Tencent Cloud provides Data Security Audit (DSA), an AI-powered database security auditing system. DSA supports comprehensive auditing of session information, access operations, and SQL statements across enterprise networks, leveraging multiple rule libraries and threat detection engines to identify malicious behaviors and promptly notify administrators to take appropriate security measures.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		services, a financial institution should adopt the appropriate digital rights management mechanism to preserve the confidentiality of its proprietary and customer information.	Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access Customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with applicable laws and regulations during investigations by national or local authorities. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities. Additionally, Tencent Cloud deploys DLP tools on employee computers to restrict external data export and monitor, detect, and prevent potential data exfiltration attempts.
13	Security Operations Centre (SOC)	(a) A financial institution should understand the scope of cloud service providers' responsibility for cybersecurity monitoring and adapt its SOC strategy and processes to ensure proactive and holistic monitoring of its cybersecurity posture. This adaptation should include the ability to effectively improve cybersecurity telemetry and analysis to detect and respond to cyber threats. (b) Where applicable, the responsibilities of cloud service providers with respect to SOC operations should be formalised in the agreement or arrangement between the financial institution and the cloud service providers, including the retention period required for relevant logs	Customers should be aware of the responsibilities of the cloud service provider in terms of network security monitoring and adjust the strategy and processes of its security operation center. Customers should conduct continuous and proactive monitoring and detection of abnormal activities in the technical infrastructure, and take appropriate responses. Additionally, customers should sign a contract agreement with the cloud service provider regarding the responsibilities for the operation of the security operation center. Tencent Cloud provides online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms

No.	Domain	Summary of Controls	Tencent Cloud's Response
		needed for forensic purposes and the right of the financial institution to access the logs for quick restoration as and when needed.	and conditions. Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Empowered by Threat Intelligence Center (TIX), Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable. For more detailed information on SOC, please refer to the content of Clause "C Security Operations Centre (SOC)" in Section 9.7 "9.7 Control Measures on Cybersecurity".
14	Cyber response and recovery	(a) A financial institution should enhance existing cyber crisis management policies and procedures to remain in a state of readiness to respond to cyber threats in a cloud environment. (b) A financial institution should extend its Cyber Incident Response Plan (CIRP) to include adverse scenarios that may affect cloud services and establish clear roles and responsibilities between the financial institution and cloud service providers for incident response and remediation. The incident escalation process and	Customers should establish an incident response plan that includes the cloud environment, clearly define the roles and responsibilities of the customer and the cloud service provider in incident response and handling, and ensure that joint business continuity tests and cyber drills with the cloud service provider are conducted to verify the effectiveness of the incident response plan. To support rapid detection and response, Tencent Cloud has established an Information Security Incident Management Standard, defining reporting, response, and handling mechanisms, as well as roles and responsibilities for each team. Tencent Cloud records security incidents in its internal security operations system. For detected incidents, Tencent Cloud analyzes and classifies them based on nature,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		turnaround time should be established with cloud service providers and periodically reviewed, to achieve an effective incident response. (c) A financial institution should consider the following additional measures in the development of its CIRP: i) enhance its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web; ii) provide adequate assistance to customers in the event of a security breach in view that the complexity of cloud arrangements and sophistication of cyber-attacks often exceed the response range reasonably expected of customers; and iii) ensure CIRP is ready to manage cross-border incidents where the data resides in a foreign jurisdiction. (d) A financial institution should ensure that relevant Cyber Emergency Response Team (CERT) members are conversant with the CIRP covering cloud services to effectively activate the CIRP when incidents occur. (e) A financial institution should extend its existing incident reporting requirements to include cloud	data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. The Tencent Cloud security team operates a 24/7 security operations framework focused on vulnerability monitoring, intrusion tracing, and attack mitigation, enabling real-time alert response and rapid development of incident containment and emergency response plans. 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 develops disaster recovery drill plans based on its Business Continuity Plan (BCP), conducts risk assessments for drills, and implements safeguards to prevent negative service impacts. Disaster recovery drills often simulate real-world scenarios, including attack-defence exercises and large-scale failures, to comprehensively validate system resilience, response speed, and recovery capability. 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 detailed information on cyber response and recovery, please refer to the content of Clause "11.12-11.16 Cyber Response and Recovery " in Section 9.2 "9.2 Cybersecurity Management".

No.	Domain	Summary of Controls	Tencent Cloud's Response
		services. (f) A financial institution should enter into agreements or arrangements with its cloud service providers to conduct integrated business continuity testing and cyber drill in accordance with the requirement on testing of disaster recovery plan in paragraph 9.48 and 9.50 of the Bank's policy document on Business Continuity Management (BCM) and paragraphs relating to cyber response and recovery under this policy document to test the effectiveness of the financial institution's CIRP and recovery plan. (g) A financial institution should review its loss provision arrangements to ensure its adequacy to cover cyber incidents in accordance with the requirement on paragraph 11.17 of this policy document.	

10

How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Electronic Know-Your-Customer ("e- KYC")

Supported by further technological advancements and introduction of electronic Know-Your-Customer (e-KYC) solutions for the financial sector, digitalisation of the customer identification and verification processes has become an increasingly prominent enabler in the onboarding process for financial services. Growing adoption and understanding of e-KYC solutions in the financial sector, the Bank Negara Malaysia officially released [Electronic Know-Your-Customer \("e-KYC"\)](#) in April 2024, enhances the existing requirements to ensure e-KYC solutions continue to remain relevant, robust and reliable.

This document expands the scope of e-KYC applications to cover both individuals and legal persons², providing guidance on e-KYC solutions that can cater to the unbanked, while ensuring uncompromised accuracy in customer identification and verification. This document sets out the minimum requirements and standards that a financial institution must observe in implementing e-KYC for the on-boarding of individuals and legal persons. It's aimed at enabling safe and secure application of e-KYC technology in the financial sector, facilitating Bank Negara Malaysia's continued ability to carry out effective supervisory oversight of financial institutions, and ensuring effective anti-money laundering, countering financing of terrorism and countering proliferation financing (AML/CFT/CPF) control measures. The requirements mainly focus on areas such as Ensuring effective e-KYC implementation, Addressing ongoing vulnerabilities, Additional safeguards to facilitate deployment, False Acceptance Rate and External independent assessment.

The Tencent Cloud [eKYC](#) solution uses Tencent's leading AI technologies in document recognition, liveness detection, and face comparison, Tencent Cloud eKYC solution simplifies the complicated traditional eKYC process into three automated steps, and accurately verifies the authenticity of user identities with the AI algorithms. Powered by a multimodal foundation model integrated with semantic understanding and self-learning capabilities, this product specifically combats deepfakes and other AIGC attacks (e.g., AI face swapping, AI expression driving), continuously enhances defense mechanisms, and accurately combats organized fraud.

The Tencent Cloud [eKYC](#) solution offers a variety of product advantages, providing customers with leading, considerate, comprehensive and secure services for verifying users' facial information, meeting the diverse facial authentication needs of customers.

- **Leading algorithms:** Tencent Cloud's face comparison algorithms have set records in multiple international contests. It achieved an industry-leading accuracy of 99.80% during LFW, which is recognized internationally as one of the most challenging face image datasets. In business scenarios, with a false accept rate (FAR) of 0.01%, eKYC has a true accept rate (TAR) over 98%.
- **High security and reliability:** The combination of liveness detection and Tencent's rich security experience and leading anti-identity attack algorithm capabilities can effectively block attacks with static photo, video reproducing, 3D-based face mask/headform and other means. It helps customers achieve business compliance and mitigate losses arising from identity frauds.

² legal person: It refers to any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLC), foundations, partnerships, or associations and other similar entities.

- **Excellent user experience:** eKYC can check whether a user's operations are proper in the course of verification and prompt the user to make adjustments via the real-time interaction, thus ensuring excellent user experience and helping improve the user's business conversion. In order to help customers better understand the operation status of the product and promptly detect any abnormalities, Tencent Cloud eKYC also provides data statistics and billing data services.
- **Easy integration:** Tencent Cloud eKYC can be easily integrated via app SDK, HTML5 or API. It can identify ID documents from multiple countries and regions, including Indonesia, Malaysia, Thailand, and Hong Kong (China), etc., providing efficient and accurate identity verification solutions to guarantee business security.

When financial institutions implement the relevant requirements in accordance with this regulatory document, Tencent Cloud, as the service provider of eKYC solutions, may participate in certain activities involved in the regulatory requirements. The following section elaborates on how Tencent Cloud, as a cloud service provider, assists financial institutions in complying with the relevant control requirements outlined in [Electronic Know-Your-Customer \("e-KYC"\)](#).

- **Due Diligence**

Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. For more details on due diligence, please refer to the content of Clause "9.2、 9.3 Assessment of service provider " in Section 5 " [5 How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing](#) ".

- **Data Availability**

The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification. To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions, organized by regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. Customers can flexibly deploy data and systems across different regions or availability zones based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures.

Tencent Cloud ensures complete isolation between different regions, maximizing stability and fault tolerance. Each region is further divided into multiple isolated availability zones to reduce the impact of single-point failures and guarantee business continuity for customers.

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.

Tencent Cloud's compute, network, storage, database, container, and middleware services provide highly available architectures and support customer-defined backup strategies to meet

diverse backup needs.

For more information related to data availability, please refer to Section 8 "[8 How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Business Continuity Management](#)", and for more information on service availability, please refer to Clause "10.32-10.35 Service Availability" of Section 9.1 "[9.1 Technology Operations Management](#)".

- **Vulnerabilities Management**

Tencent Cloud has established a threat and vulnerability management procedure to ensure timely identification of threats and vulnerabilities faced by infrastructure, information systems, etc., and to take measures to improve or repair them. Tencent Cloud regularly schedules vulnerability scans for cloud environment assets and analyzes, categorizes, and remediates detected vulnerabilities. Tencent Cloud also conducts full-chain large-scale penetration tests to proactively identify and fix potential security risks and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated via security tickets to responsible departments for timely remediation or compensating controls. After internal review by the relevant team, Tencent Cloud will promptly notify customers of the vulnerability-related information through official website announcements, internal messages, etc. The notification content includes but is not limited to the description of the vulnerability, the scope and degree of impact, the control measures already taken by Tencent Cloud, the repair suggestions proposed for customers, and specific operation guidelines.

Moreover, Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.

Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.

- **Product Testing and Independent Assessment**

To support customers in meeting regulatory requirements, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams.

Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization.

To ensure that the eKYC solution can meet the requirements of the Malaysian National Bank, Tencent Cloud invites a third-party testing agency to conduct independent tests on the eKYC solution in accordance with the requirements of ISO/IEC 30107-1³ and ISO/IEC 30107-3⁴, and issue an official test report.

³ ISO/IEC 30107-1:2023: Information technology — Biometric presentation attack detection — Part 1: Framework

⁴ ISO/IEC 30107-3:2023: Information technology - Biometric presentation attack detection - Part 3: Testing and reporting

11

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

Digital revolution has enabled a new era of connectivity, convenience and innovation. Consequently, there are more capital market entities leveraging technologies to carry out their activities in recent years. To further strengthen the ability of capital market entities to detect and mitigate risks that come with greater technology adoption, the Securities Commission Malaysia released [Guidelines on Technology Risk Management](#) in 2023, which introduce a comprehensive regulatory framework for the management of technology risk in capital market entities. The outcome desired by the SC for the Guidelines is for all capital market entities to have a robust and sound technology risk management framework which promotes strong oversight of technology risk in the capital market entity, and ultimately for the capital market to be cyber resilient. The requirements mainly focus on areas such as Governance, Technology risk management, Technology operations management, Technology service provider management, and Cybersecurity management.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in Guidelines on Technology Risk Management, and explains how Tencent Cloud, as a cloud service provider, assists capital market entities in complying with these requirements.

11.1 Governance

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.05	Cybersecurity Awareness and Training	5.05 A capital market entity must ensure that its board, senior management, employees and agents, if any, attend cybersecurity awareness training programme at least annually to enhance their awareness and preparedness to deal with a wide range of cyber risk and to carry out their respective roles effectively.	Customers should ensure that the board of directors, senior management, and employees attend at least one cybersecurity awareness training session each year. Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements. Tencent Cloud integrates information security management into daily operations to ensure employees understand and comply with internal policies and requirements.
5.06-5.09	Technology Audit	5.06 A capital market entity must— (a) establish a technology audit plan that provides appropriate coverage of critical	Customers should formulate a technology audit plan covering critical technological areas and conduct regular technology audits to ensure that the information system complies with applicable laws and regulations, that data and information are confidential, integrity and available, and that

No.	Domain	Summary of Controls	Tencent Cloud's Response
		technology; and (b) carry out its technology audit regularly. The frequency of the technology audit should commensurate with the business model, risk appetite and level of technology dependency of the capital market entity. 5.07 At the minimum, the technology audit carried out by a capital market entity must determine whether its— (a) information systems are in compliance with applicable laws, regulatory requirements and industry guidelines; (b) data and information have appropriate level of confidentiality, integrity and availability; and (c) IT service operations are being managed efficiently, and its effectiveness targets are being met. 5.08 A capital market entity must ensure that the auditors performing its audit possess the necessary competency, knowledge and experience to carry out the technology audit. 5.09 A capital market entity must— (a) ensure that the technology audit report comprises, at a minimum, independent and objective opinion on the effectiveness of risk management, governance and internal controls of the capital	the IT service operation is efficiently managed. Additionally, customers should ensure that the personnel conducting the audits possess the professional capabilities and experience related to technology audits. The audit results should be reported to the board of directors. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		market entity relative to its existing and emerging technology risk; and (b) report the outcome of its technology audit to the board.	

11.2 Technology Risk Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
6.01-6.03	Policies and Procedures	6.01 A capital market entity must establish and implement robust and effective TRM Framework to manage its technology risk effectively. The TRM Framework must be reviewed and updated periodically, and in any event, at least once in every three years by the capital market entity.	Customers should establish a technology risk management framework and conduct a review and update at least every three years. Additionally, customers should formulate policies and procedures that support the technology risk management framework. Such procedures should be reviewed and updated at least once a year. Furthermore, customers should implement internal compliance processes to ensure compliance with the technology risk management framework and related procedures.
		6.02 A capital market entity must establish and implement comprehensive and effective policies and procedures to support the TRM Framework. The policies and procedures must be reviewed and updated at least annually by the capital market entity.	Any deviations should be approved by the management. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy.
		6.03 A capital market entity must establish an internal compliance process to ensure compliance with its TRM Framework, policies and procedures. The internal compliance process must include an appropriate approval process where—	
		(a) the approval of senior management must be obtained	The Tencent Cloud security team continuously monitors and assesses internal security risks to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		prior to any deviation from its TRM Framework, policies and procedures of the capital market entity; and (b) the approval for deviation must only be given by the senior management if the deviation is supported by— (i) an appropriate justification; (ii) alternative solution or a reasonable timeframe to comply with its TRM Framework, policies and procedures.	maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. For any identified deviations, the team analyzes actual or potential causes, evaluates the need and priority for corrective and preventive actions, and implements these measures upon obtaining the necessary approvals. A dedicated oversight group tracks and records the effectiveness of corrective actions.
6.04-6.07	Technology Risk Management	6.04 A capital market entity must establish and implement its technology risk management framework comprising risk identification, risk assessment, risk mitigation, and risk monitoring, review and reporting on any existing and emerging technology adopted by the capital market entity. 6.05 A capital market entity must ensure that— (a) all risks are assigned to the appropriate risk owners who shall be accountable for ensuring that proper risk treatment plans are implemented and enforced for a specific technology risk; (b) the risk owners establish appropriate, effective and efficient technical and organisational measures in all steps of the process; and	Customers should establish a technology risk management framework, identify and assess risks, clearly define the responsible persons for risks, formulate and implement risk response measures for identified risks, evaluate remaining risks, and conduct continuous monitoring of risks, and maintain the technology risk register. To support customers in meeting regulatory requirements, Tencent Cloud has established an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. • Risk Identification: Tencent Cloud conducts risk assessments regularly, identifying applicable risk scenarios from sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk databases. Risks are identified based on these scenarios and process analysis of business products or services. • Risk Assessment: Tencent Cloud evaluates asset value, the likelihood of risk scenarios,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(c) any residual risk arising from threats and vulnerabilities after risk treatment, shall be documented and managed by risk owners according to the defined risk acceptance criteria that commensurate with the capital market entity's risk tolerance level. 6.06 A capital market entity must maintain a board-approved key technology risk register to facilitate the monitoring and reporting of technology risk. 6.07 A capital market entity must continuously review its risk exposures and associated controls to ensure that they remain in line with the risk appetite of the capital market entity.	and the potential impact, then calculates the risk level. Risk Treatment: Based on the risk analysis results, Tencent Cloud applies appropriate strategies and mitigation measures. For high-risk items, the risk owner develops a risk treatment plan (e.g., risk transfer or risk reduction measures) and updates the risk management register. For medium-risk items, the risk owner determines whether a treatment plan is necessary based on the actual environment. Low-risk items are considered acceptable risks. Residual risks are reviewed annually, and their status and risk values are monitored. Risk Monitoring, Review, and Reporting: Tencent Cloud consolidates risk assessment results into a risk assessment report for management review. The risk management register is maintained to monitor changes in risk conditions and the status of treatment plans, enabling real-time adjustments to the risk management plan. Tencent Cloud defines Key Risk Indicators (KRIs), measures them regularly, compares results against acceptable risk criteria, analyses root causes of identified issues, and proposes improvement recommendations and solutions. Furthermore, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices.

11.3 Technology Operations Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.06	System Development Life Cycle	7.06 A capital market entity must establish and implement clear requirements and	Customers should establish and implement clear system development life cycle management requirements and processes, formulate standards

No.	Domain	Summary of Controls	Tencent Cloud's Response
	(SDLC)	processes to manage its system development life cycle (SDLC) encompassing planning, requirement analysis, design, implementation, testing and acceptance. It must include, among others, requirements and processes for— (a) vendor selection and evaluation of the systems to be procured from all vendors or solution providers; and (b) assessment of software development by vendors and in-house developer, to ensure that security of the capital market entity is not compromised, and its quality assurance is met.	and procedures for supplier evaluation and selection, and assess the software development of both suppliers and internal developers. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests and, upon customer requirements, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. For more details on due diligence, please refer to Section 5 "How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Outsourcing" clause "9.2, 9.3 Assessment of service provider". Tencent Cloud integrates the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System into the entire secure product development lifecycle. This approach covers all stages—requirements, design, development, testing, delivery, and operations—embedding information security and privacy protection principles throughout the product lifecycle to ensure robust security controls and assessments. For third-party product usage, Tencent Cloud has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies.
7.07	Source Code Management	7.07 Where feasible, a capital market entity should enter into a source code escrow agreement to ensure the source codes for critical systems are	Customers should sign a source code escrow agreement to ensure that the source code of critical systems can be accessed. If the escrow agreement cannot be implemented, customers

No.	Domain	Summary of Controls	Tencent Cloud's Response
		accessible. If an escrow agreement cannot be implemented, a capital market entity must identify an appropriate alternative.	should adopt an alternative solution. All self-developed project source codes of Tencent Cloud are stored in designated code repositories. It is prohibited to store or transmit software through any external network IM, cloud storage, or code platforms. Access permissions for different roles are allocated based on scenarios and the principle of minimum authorization. For employees who change positions or have their job responsibilities adjusted, the access rights to the project repositories should be promptly revoked and the local saved code should be cleared. Tencent Cloud offers multiple storage and database services with built-in backup capabilities which can meet customers' needs for backing up their source codes, such as: • <u>Cloud Object Storage (COS)</u>: Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS)</u>: Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS)</u>: Offers scheduled snapshot capabilities for flexible backup task configuration.
7.08 、 7.09	Security Requirements	7.08 A capital market entity must— (a) incorporate security requirements into the system design which would enable it to carry out constant security evaluation; and (b) comply with security	Customers should incorporate security requirements during the system design phase and adhere to security practices throughout the entire SDLC process, in order to minimize system vulnerabilities, reduce risks, and continuously conduct security assessments. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a

No.	Domain	Summary of Controls	Tencent Cloud's Response
		practices throughout the SDLC in order to minimise system vulnerabilities and reduce risk exposure.	comprehensive Information System Secure Development Standard and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the secure product development lifecycle. This approach covers all phases—requirements, design, development, testing, delivery, and operations. At each stage, Tencent Cloud involves security teams to validate security requirements, ensuring that cloud products receive adequate security controls and assessments throughout their lifecycle, thereby reducing information security and privacy risks.
		7.09 At the minimum, the security requirements must cover main control areas including access control, authorisation, data integrity and confidentiality, logging system activity, tracking security event and exception handling.	Tencent Cloud incorporates both functional and non-functional requirements during each product iteration, drawing from sources such as user feedback, project stakeholders, product brainstorming sessions, and operational activities. During the requirements analysis phase, Tencent Cloud conducts security requirement analysis and business risk assessment. The project manager invites relevant teams—such as testing and security teams—to perform a security review of the product requirements specification. This process involves discussions on business content, workflows, and technical architecture to identify the optimal approach for embedding security. Security requirements include, but are not limited to, identity and access management, data security, network security, and security auditing.
7.10-7.15	System Testing	7.10 A capital market entity must establish a methodology for rigorous system testing and ensure that adequate testing is performed prior to deployment of a system so that the system meets its user requirements and performs as intended. At the minimum, the testing	Customers should establish a system testing mechanism to ensure that thorough testing is conducted before the system deployment. The internal testing should at least include functional testing, security testing, stress testing, etc. The problems identified during the testing process should be fully recorded and tracked, and rectification should be completed before the system is deployed to the production

No.	Domain	Summary of Controls	Tencent Cloud's Response
		conducted must cover the business logic, function, controls and performance of the system under various load and stress conditions.	environment. Tencent Cloud provides Penetration Testing Service (PTS) , which simulates real business scenarios with massive user traffic to comprehensively validate system availability and stability. PTS supports multi-region traffic generation with millions of concurrent requests and offers features such as traffic recording, scenario orchestration, traffic customization, and advanced script configuration. These capabilities enable Customers to quickly define stress test scenarios based on business models, accurately replicate large-scale application access patterns, and identify potential performance issues in advance.
		7.11 Where feasible, a capital market entity should use automated testing methodology to ensure comprehensiveness of the testing scopes, as part of the testing strategy.	To support customers in meeting regulatory requirements, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams.
		7.12 A capital market entity must properly document, track and address the issues identified during testing, including vulnerabilities, deficiencies, system defects or software bugs.	
		7.13 A capital market entity must ensure that all issues which could have an adverse impact on the operations of the capital market entity or delivery of its services to its clients are reported to the senior management and rectified prior to deployment of the system to the production environment of the capital market entity.	
		7.14 To ensure that the system is production ready and satisfies all documented requirements, a capital market entity must perform— (a) final acceptance testing including quality assurance testing focusing on technical aspect of the system; and	Tencent Cloud's change and release management process covers changes to applications, configuration files, operating systems, and databases. All changes must undergo independent functional testing before deployment. After implementing changes, Tencent Cloud's business team performs critical path regression validation to ensure changes meet expectations and do not introduce abnormal behaviour or performance

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(b) user acceptance testing focusing on functional aspect of the system. 7.15 The results of the final acceptance testing and user acceptance testing must be reported to senior management.	degradation, thereby maintaining overall system stability and availability. After release, requesters must perform post-deployment acceptance testing, and Tencent Cloud operations team monitors changes in the production environment and records results. For application security scanning, Tencent Cloud requires business teams to connect web application test environments to web vulnerability scanning tools for automated scanning before product launch. If vulnerabilities are detected, tickets are automatically generated and assigned to the responsible development team for remediation prior to release, ensuring security issues are not carried into production.
7.16	Acquired System	7.16 In the case of an acquired system, after attending to the changes during testing by a vendor, a capital market entity must ensure that the final approved version of the acquired system is used for implementation.	Customers should ensure that for the acquired system, after the manufacturer completes the revision based on the test results, customers should implement it using the final approved version. To support customers in meeting regulatory requirements, Tencent Cloud has established release and deployment management standards. These standards include creating release plans to organize the software release process in a controlled manner, deploying release packages to target environments under managed conditions, reducing risks during release and deployment, minimizing impact on production operations, and ensuring business continuity. Additionally, Tencent Cloud performs integrity checks on software packages after they are uploaded to the production environment and applies version control to maintain software package integrity and traceability. For third-party product usage, Tencent Cloud has defined software supply chain security management requirements, mandating security admission reviews for external components, security hardening and defence before

No.	Domain	Summary of Controls	Tencent Cloud's Response
			deployment, and post-launch continuous security operations and inspections. Tencent Cloud promptly addresses security issues, evaluates security posture, identifies risks, and works with vendors to implement improvements while reviewing future cooperation strategies.
7.17 、 7.18	Access Control Management	7.17 To minimise risk of unauthorised access to information assets, a capital market entity must— (a) establish user access management policies and procedures for providing, modifying and revoking access rights to IT systems. Access rights and privileges shall be granted in accordance with the roles and responsibilities of the users, and the access matrix should be periodically reviewed; (b) enforce and review its password controls periodically to enhance the resilience of its system against any attack; and (c) ensure that the logging facility is enabled to capture system user login, system activities, privilege accounts and service accounts for the purpose of audit and investigation. A capital market entity is also expected to review logs on a regular basis for any irregularity. 7.18 A capital market entity must use strong fraud deterrents for sensitive system functions to safeguard the systems and data from unauthorised access on a best	Customers should establish appropriate identity verification and access control mechanisms to manage access to information assets, and establish effective password rules. Customers should also log all access records and user management activities for all users, facilitating audits and investigations. <u>Cloud Access Management (CAM)</u> helps customers securely and granularly manage access to Tencent Cloud products and resources. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. CAM also supports viewing and tracking employee operation records through <u>CloudAudit</u>. In addition, Tencent Cloud provides <u>Bastion Host (BH)</u>, which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. To support regulatory compliance, Tencent Cloud has also established internal access control authorization policies and a role-separation matrix. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud uses a zero-trust security management system to authenticate employee access, requiring users to complete two-factor authentication through the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		effort basis. For example, the use of multi-factor authentication (MFA) and privilege access management to secure employee and customer authentication process.	system before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions to employees only based on job responsibilities and business necessities. Regular permission reviews are conducted to prevent permission misuse and abuse. Tencent Cloud implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the IT security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. Tencent Cloud has established strict management controls for privileged access. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team.
7.19 、 7.20	Cryptography	7.19 A capital market entity must implement suitable and effective cryptographic controls to safeguard the confidentiality, authenticity and integrity of its sensitive data from unauthorised access and unintentional disclosure. 7.20 A capital market entity must establish robust and sound policies and procedures to manage the use of cryptography including: (a) cryptographic key life cycle management from generation	Customers should implement international standard cryptographic algorithms. All cryptographic algorithms should undergo rigorous testing and evaluation, and a cryptographic key management policy, standard and procedure should be established covering key generation, distribution, installation, update, revocation, recovery and expiration, etc. In terms of data storage protection, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength encryption algorithms. Integrated Key Management Service (KMS) ensures full lifecycle management of encryption keys, safeguarding data confidentiality.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		to disposal; (b) measures to protect the cryptographic key from use by unauthorised parties; (c) measures to protect the cryptographic key from being modified, compromised or destroyed during its lifetime; and (d) procedures to ensure the cryptographic key is available to authorised parties only when needed with appropriate authentication and control mechanisms.	For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations. To help customers protect the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS). KMS enables customers to easily create and manage keys, meeting multi-application and multi-business key management needs while complying with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, allowing customers to apply encryption effortlessly. KMS is built on FIPS 140-2 certified Hardware Security Modules (HSMs) for key generation and protection, uses secure data transmission protocols, and employs a multi-data-center distributed cluster architecture with hot backups. Underlying HSM devices are deployed with dual-site cold backups to ensure high availability of the key management system. Regarding internal encryption key management, Tencent Cloud has established encryption and key management standards that govern the processes of key application, generation, storage, usage, transmission, rotation, and destruction to ensure the confidentiality, integrity, and availability of keys. For more details on key management, please refer to Clause "10.20-10.23 Cryptography" of Section 9.1 "9.1 Technology Operations Management".
7.21 、 7.22	Data Security	7.21 As part of its technology risk management, a capital market entity must implement effective measures to prevent	Customers should establish a data security management mechanism covering the entire lifecycle of data, including identification, processing, transmission, movement,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		losses arising from data breach or other acts of internal or external threats, negligence and cyber attack. 7.22 The measures must cover the process of identification, handling, transmission, movement, destruction and availability of data based on the following— (a) maintain a comprehensive and updated inventory of all information assets including data classification and risk across the capital market entity; (b) deploy adequate security measures to safeguard IT systems residing in the production environment, non-production environment and all other media; (c) implement appropriate controls to ensure no unauthorised person is able to access data and IT systems. Access to data and IT systems should be on a need-to-have basis; (d) implement clear desk policy to ensure information assets are not left unprotected which could potentially lead to security breaches; (e) review audit logs or trails particularly on access to critical data to identify anomalies or abnormal activities; (f) enhance monitoring and	destruction and availability. This includes maintaining an inventory of information assets, implementing security protection for IT systems, establishing access control mechanisms, enforcing desktop cleaning policies, reviewing audit logs, enhancing third-party monitoring, verifying policy processes, and managing data leakage. The <u>Data Security Governance Center (DSGC)</u> helps customers automatically identify and classify cloud-based data assets and assess associated security risks. DSGC is an integrated data security operations platform that supports sensitive data discovery, classification and grading, data mapping, and abnormal access analysis. It works in coordination with Tencent Cloud's security capabilities to form a closed-loop data protection framework, maximizing security effectiveness for enterprises. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. For asset management, Tencent Cloud has established information asset management standards and lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems. To implement network perimeter protection,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		assurance activity over third parties to ensure data and information assets of the capital market entity are adequately protected; (g) conduct a periodic gap analysis at least once a year on data and information assets processes and controls to improve data security; (h) establish a remediation plan to prioritise rectification according to the capital market entity's risk assessment; and (i) develop, operate, manage and test the data breach management processes which should include the process for preparation, identification, containment, eradication, recovery and lesson learned from data breaches.	Tencent Cloud offers a variety of services to customers, such as EdgeOne (EO) platform, Cloud Firewall (CFW), Web Application Firewall (WAF), Anti-DDoS, etc. For more detailed information on network security, please refer to the content of Clause "10.36-10.43 Network Resilience" in Section 9.1 "9.1 Technology Operations Management". Tencent Cloud has established network security management standards and a defense-in-depth architecture. Security domains are defined based on business functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time. In terms of data access control, 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. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities. Additionally, Tencent Cloud deploys DLP tools on employee computers to restrict external data export and monitor, detect, and prevent potential data exfiltration attempts. For the log auditing of access behaviors, Cloud Access Management (CAM) supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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 implements real-time security monitoring of employee account login activities. If any abnormal login behaviour is detected, the IT security system immediately contacts the account owner for verification and remediation, while recording detailed information about the incident. The production environment is fully equipped with bastion hosts, which centrally manage administrator account permissions for Tencent Cloud backend system components. Internal operations personnel must obtain approval before accessing the bastion host, and only designated Tencent Cloud staff are permitted to log in, which requires multi-factor authentication. Operation logs are centrally stored on a logging platform and regularly reviewed by Tencent Cloud's internal audit team. In terms of physical security in the office area, Tencent Cloud requires its employees to properly store paper documents containing sensitive information. After using public areas such as meeting rooms and training classrooms, employees must promptly erase confidential and sensitive information from whiteboards, turn off projectors, and retrieve meeting materials to prevent the leakage of confidential and sensitive information. A screen lock policy is implemented on Tencent Cloud employees' terminal devices to ensure the devices are locked when left unattended. Unattended equipment including copiers, fax machines, shredders, and printers is placed in monitored and appropriate locations within office areas to prevent unauthorized use and intrusion. In terms of regularly conducting gap analyses and risk assessments of processes and procedures, Tencent Cloud security team

No.	Domain	Summary of Controls	Tencent Cloud's Response
			continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. For incident management, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. For security incidents that may affect customers, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses.
7.23 、 7.24	Data Loss Prevention	7.23 A capital market entity must establish appropriate data security measures to protect the confidentiality, integrity and availability of its critical data and this should include data stored in cloud or where blockchain-based application is used. 7.24 A capital market entity must establish and implement data loss prevention (DLP) policy and procedures to safeguard: (a) Data in-use – data being accessed and processed by a system. (b) Data in-motion – data being transferred over the network.	Customers should formulate and implement data protection policies and procedures to safeguard the confidentiality, integrity and availability of data in use, during transmission and data at rest. Tencent Cloud provides Data Security Audit (DSA), an AI-powered database security auditing system. DSA supports comprehensive auditing of session information, access operations, and SQL statements across enterprise networks, leveraging multiple rule libraries and threat detection engines to identify malicious behaviors and promptly notify administrators to take appropriate security measures. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees will never access Customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or in compliance with applicable

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(c) Data at-rest – data stored in mediums such as servers, backup media, storage platform and databases.	laws and regulations during investigations by national or local authorities. Tencent Cloud enforces end-to-end identity verification and maintenance of data access permissions to ensure data integrity and service reliability. Real-time monitoring and interception mechanisms are in place to detect and block abnormal data access activities. Additionally, Tencent Cloud deploys DLP tools on employee computers to restrict external data export and monitor, detect, and prevent potential data exfiltration attempts. To ensure confidentiality and integrity of Customer data during storage, Tencent Cloud's storage and database products support encryption using secure, high-strength algorithms and integrate with the Key Management Service (KMS) for full lifecycle key management. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission.

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.26	Data Storage Capacity	7.26 A capital market entity must undertake a storage capacity assessment periodically to determine its current and future storage capacity and utilisation. If the results of the assessment warrants for a migration, a capital market entity must develop and execute a plan to migrate its data and IT systems into a new environment.	Customers should continuously monitor system resource utilization, set performance and capacity thresholds, and implement necessary processes to manage situations where predefined thresholds are exceeded. To support customers in efficient capacity planning and adjustment, Tencent Cloud provides Auto Scaling (AS) services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs, policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. To enable effective monitoring and management of system performance, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels. To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track

No.	Domain	Summary of Controls	Tencent Cloud's Response
			real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services.
7.27	Data Storage Period	7.27 A capital market entity must determine the appropriate retention period to archive its data based on the usage requirement or its criticality for its data.	Customers should determine the appropriate data archiving and retention period based on the usage requirements or criticality of the data. The variety of storage and database products offered by Tencent Cloud all allow customers to configure their own strategies for the retention period of their systems and data, meeting various data storage requirements of customers. When customers use Cloud Object Storage (COS) for file archive management, customers need to save all historical versions of files for a long time according to the compliance requirements in financial, medical, and other industries. In this case, customers can configure the lifecycle to transition and store the historical versions of files in the ARCHIVE storage class. Data lifecycle management is an advanced data management feature provided by Tencent Cloud Cloud File Storage (CFS) to balance high performance and low cost in large-scale file storage. With this feature, customers can set custom data lifecycle management policies, and the file system can automatically move cold data to lower-cost IA storage based on these policies. When the data is accessed, it is automatically restored to file storage, with the entire process being transparent to the business. If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored.

No.	Domain	Summary of Controls	Tencent Cloud's Response
7.28	Data Backup	7.28 A capital market entity must ensure data is protected by an adequate backup schedule and perform regular testing according to the needs of the capital market entity and ensure data can be restored from backups.	Customers should establish a backup management system and conduct regular backup and restoration tests. Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customer needs, such as: • <u>Cloud Object Storage (COS)</u>: Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • <u>Cloud Block Storage (CBS)</u>: Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • <u>Cloud File Storage (CFS)</u>: Offers scheduled snapshot capabilities for flexible backup task configuration. • <u>Cloud Native Database TDSQL-C</u>: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • <u>TencentDB for MySQL</u>: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • <u>TencentDB for MongoDB</u>: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios.
7.29-7.33	Data Disposal	7.29 A capital market entity must establish and implement appropriate policies for the	Customers should formulate and implement a data disposal policy to handle the data within the IT system, as well as on personal devices and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		disposal of data on its IT systems, mobile devices and storage media to safeguard the data from unauthorised disclosure.	mobile devices, ensuring that the data is irrecoverably destroyed. For third parties who have access to the data, appropriate and secure methods should be used for data cleaning, and this requirement should be included in the contract with the third party.
		7.30 A capital market entity must dispose the data kept in its IT systems when it is no longer required for business usage, legal or contractual purposes for which it was originally created or held.	Tencent Cloud manages and disposes of media based on the sensitivity of the information stored in them, and has established relevant procedures for media management. Specific processes and standards for media storage and disposal have been clearly defined. Before disposing of the media, relevant approvals are required, and records of the disposal are made. Depending on the material, storage principle, and sensitive information level of different media, the relevant teams will choose targeted handling methods to ensure that the data cannot be recovered and is in line with security standards.
		7.31 Where a capital market entity has decided that data kept in its IT devices, such as Bring-Your-Own-Device (BYOD) or corporate mobile devices, is to be disposed, the capital market entity must ensure its data will be deleted from those devices after such data is no longer in use.	When transmitting information using physical media, Tencent Cloud tracks the entire process of media outflow, transportation, and re-entry through work orders. During transportation, Tencent Cloud selects secure and reliable transportation companies and implements protective measures according to the information level. Physical media are protected and packaged to avoid physical damage during transportation.
		7.32 A capital market entity must implement a clear data sanitisation procedure to ensure data is irretrievably destroyed from its IT systems and IT devices. The data sanitisation procedure of a capital market entity must include—	For data deletion and destruction, Tencent Cloud provides secure and reliable data erasure mechanisms. Upon service termination, Tencent Cloud will apply strict data erasure procedures. After the retention period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable. When media used to provide Tencent Cloud services fails or reaches end-of-life, Tencent Cloud performs secure physical destruction following strict procedures.
		(a) record data sanitisation activities performed such as location of the IT systems and IT devices, sanitisation date and name of responsible individual(s); and	
		(b) clear identification of data accessible by a third party and access controls to address the risk of third-party having	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		access to data that is not appropriately disposed.	
		7.33 A capital market entity must require all third parties who have the data of the capital market entity in its custody to perform data sanitisation appropriately and securely to avoid the risk that the data that is no longer in use to be accessible by a third party. A capital market entity should include such requirements in any contract entered into with a third-party service provider.	
7.34-7.37	Change Management	7.34 A capital market entity must establish a change management process to oversee any changes made to its IT systems covering among others, impact assessment, approval, scheduling, implementation and communication to key stakeholders. 7.35 A capital market entity must ensure, prior to deploying any changes to its IT systems in the production environment— (a) a risk and impact analysis is conducted on all proposed changes to the IT systems. This risk and impact analysis should be included in the test plans of the capital market entity; (b) the analysis takes into account security factor and implication of the change in relation to the capital market entity's other IT systems;	Customers should establish a change management procedure to ensure that any changes to information assets are assessed, tested, reviewed, and approved prior to implementation, and establish and implement a clear emergency change handling process. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also maintains an emergency change management process, under which emergency changes must receive appropriate approval before execution. All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(c) the results of the analysis are accepted and approved by senior management; (d) all key stakeholders (comprising the relevant business groups in the capital market entity that will be affected by the proposed change) are informed and provided with recommendations on the proposed change; and (e) the IT systems configuration is backed up and a fall-back plan is prepared in case a problem arises during or after the implementation of a change. 7.36 A capital market entity must establish and implement clear process and procedures to handle any emergency change to the production environment. 7.37 A capital market entity must record activities performed during the change process in an activity log to facilitate investigation and troubleshooting.	detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment. Tencent Cloud classifies change requests based on attributes such as importance, urgency, and scope of impact. For changes that may affect external environments—such as product, infrastructure, or network configuration changes—Tencent Cloud will notify customers through announcements, email, the Tencent Cloud console, and/or other appropriate channels.
7.38-7.44	Patch and Technology Obsolescence	7.38 A capital market entity must establish a patch management process to administer the remediation effort, risk assessment, monitoring and implementation of security patch that is applicable to its IT systems. A capital market entity must perform patch management diligently and continuously monitor and	Customers should establish a patch management process, implementing patches based on the severity of the patches and the importance of the IT system. Before implementation, tests should be conducted. Customers should formulate a technology update plan, conducting risk assessments for software and hardware that are about to reach the EOS date, and replacing them upon expiration. If the expired software or hardware is to be used, approval from the management is required.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		implement the latest patch releases in a timely manner.	For patch management , Customers can use Cloud Workload Protection Platform (CWPP) to detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities, receive real-time alerts, and obtain remediation plans to quickly address vulnerability risks. Tencent Cloud Container Security Service (TCSS) provides a virtual patching system designed to protect against frequently occurring zero-day vulnerabilities. It integrates Tencent's vulnerability discovery and real-time high-risk vulnerability alerting technologies to capture and analyse vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically apply them to cloud servers to effectively block hacking attempts. In addition, customers can use Vulnerability Scanning Service (VSS) to perform regular security scans on enterprise network devices and application services, receive continuous risk alerts and vulnerability detection, and obtain professional remediation recommendations to reduce security risks.
		7.39 A capital market entity must closely monitor the EOS dates of its hardware and software including those relating to security vulnerabilities that surface after the EOS date.	Tencent Cloud identifies the latest patches and conducts thorough security testing before installation. Internal teams are regularly notified to apply patches, and endpoint detection tools scan patch status. Overdue patches trigger automated alerts. Tencent Cloud also operates internal vulnerability scanning and external vulnerability reporting platforms to track and remediate issues. Security tickets are logged in the operations system and assigned to responsible teams for timely resolution. Tencent Cloud's security research team integrates virtual patching capabilities into its Web Application Firewall to enhance overall platform security.
		7.40 A capital market entity must develop a technology refresh plan for the replacement of its hardware and software before they reach EOS. A capital market entity must assess the impact and include risk mitigation process should the EOS system be utilised within a certain period.	For technology End-of-life management , Tencent Cloud maintains a detailed inventory of hardware and facilities in its Configuration Management Database (CMDB), including each
		7.41 A capital market entity must ensure that its critical IT systems are not running on obsolescence systems or EOL systems. If there is a need for a capital market entity to continue using critical technology which are running on obsolescence systems, it must—	
		(a) ensure that approval is obtained from senior management and a validity period is assigned to the continued use of such critical IT systems that commensurate with the identified risks and risk mitigation process of the capital market entity; and	
		(b) closely monitor, assess the impact and establish a risk	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		mitigation process that corresponds to its risk acceptance level for such critical IT systems. 7.42 The capital market entity must ensure that the latest inventory list of all IT systems is mapped to its criticality and is available for patch administration for the purpose of determining its patches severity and for further remedial action. 7.43 A capital market entity must conduct patch compatibility testing on its IT systems that use standardised configurations before deploying to its IT systems in production environment to ensure it does not introduce any adverse effect. The patch deployment must be carried out within a specified timeframe depending on the severity level of the patch. 7.44 The capital market entity must ensure the remediation action is approved, monitored and tracked according to the change management process.	server's End-of-Support (EOS) date and version information. Tencent Cloud regularly retires and replaces servers, while software components (such as operating systems and database systems) are upgraded to appropriate versions before reaching end-of-support. For decommissioned hard drives, Tencent Cloud uses secure physical destruction methods to ensure complete disposal and records the destruction in official logs.
7.45-7.48	Network Resilience	7.45 A capital market entity must design a sound network architecture to support its business activities and future growth and to enable it to achieve high network availability, redundancy, accessibility and resiliency. 7.46 A capital market entity must continuously assess its	Customers should design and implement a robust network architecture, supporting the high availability and reliability of the network infrastructure through means such as redundancy, fault tolerance, congestion control and diversity in network routing. All changes to the network infrastructure need to be implemented through change management. To support customers in meeting regulatory requirements, Tencent Cloud operates data

No.	Domain	Summary of Controls	Tencent Cloud's Response
		network architecture design to identify any flaws and to sustain an acceptable level of availability which may support the business activities of the capital market entity. 7.47 A capital market entity must ensure its network infrastructure with systems that demand high availability and reliability to have no single point of failure by implementing redundancy, fault tolerance, congestion control and diversity in network routing, where applicable. 7.48 A capital market entity must ensure that the change management process provided in paragraph 7.34 is applicable to any changes made to the network infrastructure.	centers across multiple global regions, organized by 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 based on business continuity and data security requirements, ensuring disaster recovery capabilities. Each availability zone connects to multiple network carriers, enabling cross-region disaster recovery and reducing the impact of public network failures. Tencent Cloud's core network adopts a redundancy architecture, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services even in the event of single-point device failures. Similarly, Tencent Cloud's compute nodes use a redundancy design, where faulty nodes are automatically removed in real time by the scheduler, ensuring business availability. 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. Tencent Cloud regularly reviews its network security architecture and protection strategies, including firewall, IPS/IDS, and DDoS configurations, to identify vulnerabilities and update security rules. All network architecture and device changes follow a strict change management process, including impact analysis, rollback planning, and formal approval before implementation.
7.49-7.51	Data Centre Operation	7.49 A capital market entity must ensure that its data centre operation, including the use of	Customers should ensure that the operation of the data center is based on a robust IT infrastructure, and take necessary measures to

No.	Domain	Summary of Controls	Tencent Cloud's Response
		cloud services, is supported by a sound IT infrastructure taking into consideration IT operational resiliency and availability target that is aligned to the business needs of the capital market entity. The availability target set by the capital market entity should result in reducing the impact of any failure or disruption to the data centre operations of the capital market entity. 7.50 Where applicable, to reduce the impact of any failure or disruption to the data centre operations, a capital market entity must— (a) conduct a data centre risk assessment to ensure the resiliency of the data centre, taking into consideration the business model and risk appetite of the capital market entity, and industry best practices; (b) ensure no single point of failure (SPOF) to its critical IT infrastructure including power equipment, network connectivity, cooling equipment, electrical utility and diversification of data communication and network paths attending the IT system; (c) maintain a secondary data centre for recovery purposes based on the business needs of the capital market entity; (d) undertake a data storage capacity assessment to	reduce the risk of operational failures or disruptions in the data center. Such measures include conducting a data center risk assessment, diversifying critical IT infrastructure, establishing backup data centers, conducting storage capacity assessment and performance monitoring, maintaining the data center, establishing an emergency response mechanism for data center security incidents, and implementing access control for the data center. Additionally, if the data center is managed by a third-party service provider, customers should ensure that the provider can submit a data center risk assessment report. In 2026, Tencent Cloud launched three data centers in Malaysia. To ensure resilience and security, Tencent Cloud has built a comprehensive management system covering the entire process—from data center operator onboarding and contractual obligations to ongoing supervision. Tencent Cloud ensures that all global data centers are selected, constructed, or leased in compliance with relevant international standards and local security requirements. For leased data centers in Malaysia, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity, Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the data center. For physical access control, Tencent Cloud requires operators to establish formal access

No.	Domain	Summary of Controls	Tencent Cloud's Response
		determine its current and future storage capacity and utilisation; (e) ensure adequate maintenance of the data centres; (f) continuously monitor the data centre resources according to internal thresholds determined by the capital market entity to ensure the performance of the data centre resources are not disrupted; (g) implement an escalation process and response plan to analyse and remediate any potential or actual threats related to the data centres; and (h) implement adequate physical access controls for its data centres including process on authorised employees, visitor access and access to selected areas. 7.51 Where a third-party service provider manages the data centre, the capital market entity must ensure that the third-party service provider furnishes a data centre risk assessment report upon request by the capital market entity or the SC. The report must cover the review of the system of the data centre, suitability of its design of controls and effectiveness of the controls. The capital market entity must perform its own risk assessment of such report to ensure it is consistent with the	procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. For physical and environmental incidents, Tencent Cloud requires operators to establish escalation mechanisms, response plans, and handling procedures, and to conduct regular drills to validate these processes. This ensures rapid response and resolution of such incidents, minimizing their impact on Tencent Cloud's platform and services. During data center operations, Tencent Cloud has established a continuous monitoring and assessment mechanism to regularly evaluate operators' physical environment, technical

No.	Domain	Summary of Controls	Tencent Cloud's Response
		risk appetite and risk tolerance of the capital market entity.	capabilities, service responsiveness, and risk control effectiveness. Tencent Cloud conducts annual on-site audits to verify that data center operators comply with Tencent Cloud's information security requirements. Additionally, Tencent Cloud reviews the results of Threat and Vulnerability Risk Assessments (TVRA) performed by data center service providers to ensure the effectiveness of related management measures.
7.52 、 7.53	Capacity Management	7.52 A capital market entity must ensure that its IT system has adequate storage, central processing unit power, memory and network bandwidth to support its business operations and future growth. 7.53 A capital market entity must monitor its technology operation status including its network performance, application and system utilisation to ensure its IT resources meet its current needs and future growth, and for capacity management planning.	Customers should continuously monitor system resource utilization, set performance and capacity thresholds, and implement necessary processes to manage situations where predefined thresholds are exceeded. To support customers in efficient capacity planning and adjustment, Tencent Cloud provides Auto Scaling (AS) services. AS automatically monitors the health status of instances and adjusts cloud server computing resources based on customers' business needs, policies, and predefined scaling conditions. This ensures that an appropriate number of cloud server instances are always available to handle application workloads. To enable effective monitoring and management of system performance, customers can use Tencent Cloud Observability Platform (TCOP). This service provides real-time monitoring, analysis, and alerting capabilities for cloud products and resources. TCOP collects and visualizes monitoring metrics reported by cloud servers, cloud databases, and other cloud products, as well as custom metrics defined by customers. It helps customers track resource utilization, application performance, and the operational status of cloud products in real time. Customers can configure alerts based on specific metrics, and receive timely notifications of business anomalies via message push and other channels.

No.	Domain	Summary of Controls	Tencent Cloud's Response
			To support customers in meeting regulatory requirements, Tencent Cloud forecasts capacity needs based on business operations and formulates an annual capacity management plan. Business units, while ensuring system continuity, reference historical monitoring data to identify capacity usage trends and consider new business and system requirements to develop capacity forecasts and plans. During daily operations, Tencent Cloud teams use an internal capacity monitoring platform to track real-time utilization of underlying cloud platform services and identify usage trends. When consumption exceeds predefined thresholds, the monitoring platform issues alerts to relevant teams, prompting timely actions to ensure stable operation of products and services.
7.54 、 7.55	Security Monitoring	7.54 A capital market entity must establish a monitoring and reporting mechanism of its network, application and system to flag abnormal behaviour and aid in analysis. Upon the detection of any abnormal behaviour, the capital market entity must undertake a follow-up action in accordance with its internal procedures. 7.55 A capital market entity must retain adequate network, application and system device logs for investigation and diagnosis for an appropriate period as it determines.	Customers should establish a log management mechanism to collect, process and analyze the logs of the network, applications and system devices, identify suspicious or abnormal behaviors, and achieve timely detection and response to cybersecurity incidents. 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 alerts from cloud security products, cloud asset configuration change data, cloud user operation

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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. Tencent Cloud also operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls, and servers, and uses a ticketing system to track and resolve identified security issues. Tencent Cloud has defined detailed operational security “red lines” and, leveraging

No.	Domain	Summary of Controls	Tencent Cloud's Response
			years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts.
7.56-7.59	IT Disaster Recovery Plan (IT DRP)	7.56 A capital market entity must establish and test its IT DRP on a regular basis to manage availability and restore IT system within the recovery time objectives being set in the event of disruption according to its defined BIA. 7.57 A capital market entity must ensure that all relevant key stakeholders from business and IT functions participate in the IT DRP to ensure the IT DRP is implemented effectively. 7.58 A capital market entity must ensure that the IT DRP consists of– (a) procedures for declaring a disaster with escalation procedures; (b) criteria for plan activation (including circumstances in which a disaster is declared, type of scenarios of disasters and when the recovery plan should be put into action); (c) its linkage with overarching plans such as emergency response plan or crisis management plan for business continuity plan (BCP) for different lines of business; (d) the responsible employee for each function in plan	Customers should establish a business continuity management mechanism, conduct business impact analysis, clearly define recovery time objectives, develop and test a disaster recovery plan. If the IT system is managed by a third-party service provider, customers should ensure that the service provider has the ability to guarantee the availability and recovery capability of the IT system. The testing of the disaster recovery plan can be jointly participated in by the third party. To ensure business continuity for customers, Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud computing environment and has obtained international certification for the ISO/IEC 22301 Business Continuity Management System. Tencent Cloud performs business impact analysis for its cloud products and services, defines RTOs and Recovery Point Objectives (RPOs), and develops response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans are established for cloud products and critical processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Tencent Cloud regularly conducts business continuity drills and tests based on these plans to ensure their feasibility. If the customer assesses that the disaster recovery drill requires Tencent Cloud's participation and collaboration, Tencent Cloud will respond promptly and fully cooperate.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		execution; (e) recovery teams and their responsibilities; (f) emergency contact and notification (recovery teams, recovery manager, stakeholders, important third-party service providers); (g) a detail procedure of the recovery process (initiation of recovery place, type of recovery to be conducted, the flow of recovery); (h) identification of the various resources required for recovery and business operation continuation; and (i) post incident review incorporating lessons learned and developing long-term risk mitigations. 7.59 Where IT systems are managed by a third-party service provider, the capital market entity must ensure that the third-party service provider is capable in ensuring availability and recovery of the IT systems. The capital market entity must coordinate the DRP with involvement from the third-party service provider for such IT systems to meet the business recovery objectives.	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 8: “How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Business Continuity Management” and Section 12 “How Tencent Cloud Meets and Assists Customers to Meet the SC Requirements of Guiding Principles on Business Continuity”.

11.4 Technology Service Provider Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
8.01-	Due Diligence	8.01 A capital market entity	Customers should establish an outsourcing

No.	Domain	Summary of Controls	Tencent Cloud's Response
8.05	and Performance Monitoring	must implement and uphold robust and sound risk management in relation to its outsourced arrangements including any sub-arrangements.	management mechanism, conduct due diligence before selecting a third-party service provider, implement effective contract management and performance monitoring, and ensure that the selected third-party service provider has good network hygiene practices.
		8.02 A capital market entity must ensure that— (a) the third-party service providers it engages are reliable by conducting due diligence prior to selecting a third-party service provider; and (b) it carries out contract management and performance monitoring so as to minimise any risks related to the technology it expects to adopt from the thirdparty service provider.	In response to customer evaluations of service providers, Tencent Cloud will provide relevant information upon request and assign dedicated personnel to actively support and cooperate with customers' due diligence activities. The following is an overview of Tencent Cloud's practices as a cloud service provider in responding to due diligence requirements across various aspects:
		8.03 The scope of the due diligence to be conducted by a capital market entity pursuant to paragraph 8.02 above must include the following: (a) financial stability and reputation of the third-party service provider; (b) where applicable, the managerial skills, technical competency and operational capability of the third-party service provider; and (c) the third-party service provider's capacity to undertake the provision of the outsourced task effectively at all times.	• Reputation: As a cloud computing brand under Tencent, a leading enterprise in China's internet industry, Tencent Cloud has obtained multiple professional certifications from industry organizations, provides comprehensive cloud solutions, and has delivered reliable services to numerous enterprises and government agencies. • Financial Strength: Tencent Cloud, as a cloud computing brand developed by Tencent Group, benefits from the Group's strong financial position and stability. Since Tencent Cloud officially launched its services in 2010, it has achieved significant growth in key financial indicators such as revenue and profitability. Tencent Cloud has been recognized by Gartner for four consecutive years, ranking second among Chinese vendors in the strategic quadrant. • Technical strengths: Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity
		8.04 A capital market entity	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		must conduct periodic assessment on the capabilities of the third-party service providers during the contract period, including the third-party service provider's capability in managing risk. In assessing the capabilities of the thirdparty service provider in managing risk, a capital market entity must also consider the following factors: (a) Data loss; (b) Technology risk; (c) Reputational risk; (d) Exit risk; (e) Concentration risk; (f) Operational risk including resiliency to operational and system disruption, disaster preparedness plan and business continuity plan (BCP); (g) Data security of the capital market entity and its clients' data integrity including unauthorised access and mishandling of data and information during data-atrest, data-in-motion and data-in-use; and (h) Resiliency to cyber risk. 8.05 A capital market entity must ensure that the selected third-party service provider practices cyber hygiene and remains cognisant in protecting its data confidentiality, and the integrity and resilience of its systems.	protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and dependable cloud environment. Tencent Cloud's mature operational security capabilities enable 24/7 technical support for its cloud products, ensuring reliable and continuous service for customers. Exit plan: If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Tencent Cloud supports data migration using standard formats and the same transmission methods as during onboarding, including Direct Connect (DC) and VPN Connection, services, to ensure secure and reliable data transfer. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored. Concentration risk management: To assist Customers in addressing concentration risk, Tencent Cloud operates data centers across multiple global regions, organized into regions and availability zones, covering Mainland China, Asia-Pacific, North America, and Europe. When launching instances, customers can select any Availability Zone within a designated Region deploying instances across independent Availability Zones safeguards applications against failures in a single location. Customers can flexibly deploy data and systems across different regions or availability zones according to business development

No.	Domain	Summary of Controls	Tencent Cloud's Response
			needs and data security requirements, adopting suitable business continuity models to meet disaster recovery objectives. Business continuity management: Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, certified to ISO/IEC 22301 international standards. To ensure service availability, Tencent Cloud conducts business impact analyses to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and develops disaster recovery strategies and continuity plans accordingly. Detailed contingency plans are established for cloud products and critical processes, and regular continuity drills are performed to validate their effectiveness. Data security: To ensure confidentiality and integrity, Tencent Cloud storage and database products support encryption using strong algorithms and integrate with the Key Management Service (KMS) for full lifecycle key management. Redundant storage and erasure coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors. Cyber security risk management: Tencent Cloud develops and maintains an internal risk management framework based on the ISO/IEC 27001:2022 standard to identify, analyze, and manage recognized risks. Tencent Cloud conducts formal risk assessment regularly. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC. To ensure that Tencent Cloud's IT policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party.
8.07-8.09	Cloud Services	8.07 A capital market entity must ensure the level of governance and controls implemented over cloud service providers including cloud strategy and cloud operational management commensurate with the risks posed by the cloud services it adopts. The board of the capital market entity should be responsible and accountable for maintaining effective oversight and governance in this regard. 8.08 A capital market entity must be cognisant of and ensure risks associated with the use of cloud services are adequately addressed. It must perform a comprehensive risk assessment when planning for cloud adoption and manage the risks identified appropriately. 8.09 A capital market entity must, prior to cloud adoption,	Customers should ensure proper management of the use of cloud services, ensuring that the governance and control levels implemented by the cloud service provider are commensurate with the risks associated with using cloud services. Additionally, customers should conduct a risk assessment when planning to adopt cloud services, covering at least cloud risk management, location of cloud infrastructure, multi-tenancy situation, identity and access control, data protection and key management, public cloud network security, cloud resilience management, portability, migration to the cloud, and compliance with applicable regulatory requirements. Tencent Cloud, in accordance with contractual agreements, grants customers audit and oversight rights and provides dedicated personnel to actively support customer-initiated audits or inspections. (a) Cloud risk management strategy Tencent Cloud develops and maintains an internal risk management framework based on the ISO/IEC 27001:2022 standard to identify, analyze, and manage recognized risks. Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
		conduct a comprehensive risk assessment which addresses key risks associated with among others, the following: (a) Cloud risk management strategy, considering different cloud service models tailored to their needs; (b) Location of the cloud infrastructure; (c) Multi-tenancy or data commingling; (d) Identity and access management (IAM) controls, data protection and cryptographic key management; (e) Expansion of cybersecurity operations of the capital market entity including the security of public cloud infrastructure; (f) Cloud resilience risk management such as cloud redundancy or fault tolerant capability, high availability, scalability, multiple geographically separated data centres; (g) Vendor lock-in and portability or interoperability solutions; (h) Exposure to cyber-attacks via cloud service providers; (i) Migration of existing systems to cloud infrastructures; and (j) Constant ability to meet regulatory requirements and	Cloud conducts formal risk assessment regularly. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. (b) Location of the cloud infrastructure Tencent Cloud's infrastructure is deployed across multiple global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an isolated fault domain with physical separation. Customers can flexibly deploy data and systems across different regions or availability zones based on business growth needs and data security requirements to meet disaster recovery objectives. (c) Multi-tenancy or data commingling 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. (d) Identity and access management (IAM) controls, data protection and cryptographic key management For access control management, Cloud Access Management (CAM) can help the customer to assign resource permissions to sub-users through tags and other methods, achieving fine-grained access control over cloud resources. Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on

No.	Domain	Summary of Controls	Tencent Cloud's Response
		timely measures of security standards on cloud computing.	dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access assets and complete tasks. For data storage protection, Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption keys are managed through the integrated Key Management Service (KMS), which provides full lifecycle management. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. (e) Security of public cloud infrastructure Tencent Cloud ensures that all global data centers are selected, constructed, or leased in compliance with relevant international standards and local security requirements. For leased data centers in Malaysia, Tencent Cloud requires operators to implement highly stable, fully redundant power and cooling systems to guarantee continuous power and cooling even in the event of a single point of failure. Tencent Cloud also mandates that operators equip data centers with comprehensive fire protection systems, including localized fire detection systems, automatic fire suppression systems, and manual firefighting equipment for emergency use. To prevent damage caused by static electricity, Tencent Cloud requires operators to install anti-static flooring and grounding lines for racks, cable trays, and other components within the data center. (f) Cloud resilience risk management Tencent Cloud has obtained ISO/IEC 22301

No.	Domain	Summary of Controls	Tencent Cloud's Response
			certification for its Business Continuity Management System. To ensure the continuous availability of customer services, Tencent Cloud has developed detailed disaster recovery plans for its cloud products and conducts regular drills in strict accordance with requirements to ensure the timeliness and feasibility of these plans. (g) Vendor lock-in and portability or interoperability solutions If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Tencent Cloud supports data migration using standard formats and the same transmission methods as during onboarding, including Direct Connect (DC) and VPN Connection, services, to ensure secure and reliable data transfer. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored. (h) Exposure to cyber-attacks via cloud service providers 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. (i) Migration of existing systems to cloud infrastructures Cloud Migration(CMG) integrates various migration tools enables customers to quickly migrate system to the cloud. In addition, Tencent Cloud also provides Migration Solution, which help customers migrate to Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
			services efficiently at low costs, so that customers can use Tencent Cloud's powerful, secure, and stable cloud computing capabilities to grow business. (j) Constant ability to meet regulatory requirements and timely measures of security standards on cloud computing Tencent Cloud strictly complies with the laws and regulations of the jurisdictions in which it operates. 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 undergoes professional third-party audits annually.
8.10 、 8.11	Data at the Cloud	8.10 A capital market entity must assess and manage its exposure to technology risk that may affect the confidentiality, integrity and availability of the IT systems and data at the cloud during the contractual period of the cloud services agreement. 8.11 A capital market entity must ensure adequate measures are undertaken by the cloud service provider to safeguard the data of the capital market entity and the data of its clients against unauthorised disclosure and access. For encrypted data, a capital market entity must ensure that appropriate cryptographic key management is established,	Customers should assess and manage the IT systems and data in the cloud environment, ensuring that the cloud service provider takes necessary measures to protect data security and prevent unauthorized access and disclosure. For encrypted data, customers should ensure that appropriate cryptographic key management is established. For data access and protection aspects, customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. Tencent Cloud has established strict access control policies and implemented permission management and authorization mechanisms. Bastion hosts are fully deployed in the production environment to centrally manage administrator account permissions and activities for backend system components. For data storage security aspects, Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
		including assessing the ability of the cloud service provider to restore the services effectively.	Cloud storage and database products support encryption using strong algorithms and integrate with the Key Management Service (KMS) for full lifecycle key management. Redundant storage and erasure coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors. For data transmission protection, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. To assist customers in protecting the confidentiality, integrity, and availability of keys, Tencent Cloud provides the Key Management Service (KMS), which enables customers to easily create and manage keys for multiple applications and business scenarios in compliance with regulatory requirements. KMS integrates seamlessly with encryption features of services such as object storage, distributed databases, and cloud disks, simplifying encryption implementation. Regarding internal encryption key management, Tencent Cloud has established encryption and key management standards that govern the processes of key application, generation, storage, usage, transmission, rotation, and destruction to ensure the confidentiality, integrity, and availability of keys. For more details on key management, please refer to Clause “10.20-10.23 Cryptography” of Section 9.1 “9.1 Technology Operations Management”.
8.12-8.14	Contract Management	8.12 A capital market entity must establish a service level agreement when engaging third party service providers. 8.13 The service level	Customers should sign a service level agreement when cooperating with a third-party service provider, which should at least include requirements such as service scope, performance indicators, data confidentiality and security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		agreement entered by a capital market entity with its third-party service provider must at a minimum include provisions on— (a) scope of arrangement, duration of the service and performance metrics; (b) confidentiality and security requirements of the capital market entity and the data of its clients during and after the end of the contract period; (c) access rights to information or documents of the third-party service provider related to any outsourced function as may be required by the SC or the capital market entity for the purpose of performing review or audit on the relevant systems; (d) the right for the SC to appoint an independent party to perform a review or audit of the relevant information or document of the capital market entities stored with or held by the third-party service provider and the costs for such review or audit shall be borne by the capital market entity; (e) contingency plans and exit strategies with minimal impact on the continuity of the operations of the capital market entity; (f) system development and maintenance arrangements with the third-party service	requirements, audit rights, exit strategies, system development and maintenance arrangements, incident notification, and security responsibilities. Customers should regularly review whether the performance of the third-party service provider complies with the signed service level agreement and ensure that the third-party service provider complies with relevant laws and regulations. As a cloud service provider, Tencent Cloud offers online legal documents on its international portal such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, the service term, and the scenarios under which the agreements may be terminated. Customers may also choose to enter into an offline agreement with Tencent Cloud to negotiate specific terms and conditions. Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console. Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization. To ensure that Tencent Cloud's IT

No.	Domain	Summary of Controls	Tencent Cloud's Response
		provider including requirements for such third-party service provider to comply with the data and information security policies of the capital market entity; (g) a clearly defined arrangement for immediate notification by the third-party service provider to the capital market entity in the event of a technology incident or cyber incident; (h) clearly defined cyber security responsibilities of all parties; (i) modification or termination of the arrangement between the capital market entity and the third-party service provider in the event the SC issues a direction to the entity to that effect under securities laws, these Guidelines or any other relevant guidelines, guidance or practice notes; and (j) compliance with applicable laws, regulations, guidelines and requirements by the third-party service provider. 8.14 A capital market entity must— (a) periodically review the performance of its third-party service providers to ensure satisfactory performance is achieved and review the service level agreement it enters into to ensure it remains relevant and effective; and	policies, procedures, processes, and controls meet the requirements of Malaysia financial regulations, Tencent Cloud has successfully passed the IT compliance audit for the Malaysia financial industry conducted by an independent third party. Customers can independently download the latest reports from Tencent Cloud's Compliance Document Center. Tencent Cloud will, as appropriate, assign dedicated personnel to actively respond to and support audit and supervisory requirements from customers.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		(b) ensure its third-party service providers comply with all applicable laws, regulations, guidelines and requirements.	Customers should ensure that the data stored with the third-party service provider can be restored promptly. Tencent Cloud offers a wide range of products designed with high availability features to help customers achieve system and service resilience. For example: • <u>Cloud Load Balancer (CLB)</u> provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • <u>Cloud Virtual Machine (CVM)</u> ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • <u>Cloud Object Storage (COS)</u> provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for Customer data to ensure durability. • <u>TencentDB for MySQL</u> supports high reliability and availability with robust automatic backup and lossless recovery mechanisms. • <u>Tencent Kubernetes Engine (TKE)</u> uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure
8.15	Data Recovery	8.15 A capital market entity must ensure that all of its data residing with third-party service providers are recoverable in a timely manner.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and highly available services and data. Tencent Cloud ensures complete isolation between different regions, maximizing stability and fault tolerance. Each region is further divided into multiple isolated availability zones to reduce the impact of single-point failures and guarantee business continuity for customers. For more details on business continuity, refer to Section 8: “How Tencent Cloud Meets and Assists Customers to Meet the BNM Requirements of Guidelines on Business Continuity Management” and Section 12 “How Tencent Cloud Meets and Assists Customers to Meet the SC Requirements of Guiding Principles on Business Continuity”.

11.5 Cyber Security Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.03	Cyber Risk Management Strategies	9.03 As part of a wider risk management programme, a capital market entity must implement cyber risk management strategies and measures in a structured and methodical manner which includes identification, protection and prevention, detection, response and recovery measures.	Customers should implement cyber risk management strategies and measures in a structured and methodical manner. To support customers in meeting regulatory requirements, Tencent Cloud has defined an Information Security Risk Management Procedure, which provides clear guidance for the entire risk management lifecycle, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessments regularly, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Cloud's risk management requirements. Furthermore, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices.
9.04	Cyber Security Measures	9.04 A capital market entity must deploy defence-in-depth and preventive cyber security measures which commensurate with its business model, risk appetite and level of technology dependency. A capital market entity must put in place the appropriate measures which may include the following: (a) Deployment of anti-virus software and malware programme to detect and isolate malicious code; (b) Layering systems and systems components; (c) Deployment of firewalls to reduce weak points through which attacker can gain access to an entity's network; (d) Web and email filtering systems; and (e) Solution to counter advance persistent threats such as zero day and signatureless-malware.	Customers should deploy defence-in-depth and preventive cyber security measures which commensurate with its business model, risk appetite and level of technology dependency, including deploying antivirus software and malicious programs, implementing a layered system, deploying firewalls, adopting network and email filtering systems, and developing solutions to address persistent threats. In terms of antivirus and anti-malware protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to provide comprehensive monitoring and control of all server endpoint assets. The EDR solution supports antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing of command operations and login activities. It triggers alerts upon detecting malicious programs or abnormal behaviors, and Tencent Cloud follows up and handles these alerts through its ticketing system. For network segmentation or partitioning, customers can use Tencent Cloud's Virtual Private Cloud (VPC) service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access

No.	Domain	Summary of Controls	Tencent Cloud's Response
			control. To implement network perimeter protection, Tencent Cloud offers a variety of services to customers, such as EdgeOne (EO) platform, Cloud Firewall (CFW), Web Application Firewall (WAF), Anti-DDoS, etc. For more detailed information on network security, please refer to the content of Clause "10.36-10.43 Network Resilience" in Section 9.1 "9.1 Technology Operations Management". 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. For Internet browsing security, Tencent Cloud's network team has implemented multi-layered protective measures, including unified control of internet browsing channels, enabling web security filtering and malicious URL blocking, deploying endpoint security and antivirus software, and providing employees with security awareness training for safe internet browsing to protect internal networks. By deploying firewalls, anti-virus software and email gateways, real-time scanning of attachments and links, and email system patches are updated regularly to fix vulnerabilities. At the same time, log auditing function is enabled to record all sending and receiving operations. 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,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			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, 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.
9.05 9.06	Security Hardening and Configuration	9.05 A capital market entity must— (a) establish, implement and continuously review the security hardening standards on its operating systems, databases, applications, network and security devices; and (b) ensure that the security hardening standards checklist is kept updated. 9.06 A capital market entity must conduct continuous review and update of rules and configurations for its operating systems, databases, applications, network and	Customers should establish security hardening standards for the operating system, database, application, network and security devices, and regularly review the configurations to ensure the security and accuracy of the configurations. Cloud Security Center (CSC) offers automated inspection and assessment capabilities for cloud product configuration risks, helping customers mitigate security risks arising from incorrect security configurations in cloud product usage and enhance their overall cloud security posture. Meanwhile, customers can adopt Config to conduct centralized audit and governance of cloud resources. Config continuously records configuration information and configuration changes of various cloud resources across different regions under a customer's account. Based on Tencent Cloud best practice rules and compliance package templates, it automatically performs continuous compliance assessments on

No.	Domain	Summary of Controls	Tencent Cloud's Response
		security devices.	cloud resource configurations under an enterprise account, identifies non-compliant resource configurations, and thereby enables automated monitoring and management of cloud resources. To assist customers in complying with regulatory requirements, Tencent Cloud has established a configuration management system and centrally manages all IT service components and configuration items through a Configuration Management Database (CMDB). It standardizes the management of Configuration Items (CIs) and their interrelationships. If a change process involves configuration updates, O&M personnel shall update the versions and relevant information of the configuration items in the CMDB in accordance with the change plan after completing the change. Tencent Cloud conducts regular asset inventories and audits the CMDB to ensure the validity, accuracy, and completeness of all configuration item information. In addition, Tencent Cloud has formulated a set of network security configuration standards and security baseline standards, aiming to standardize the management of security configurations for network devices, firewalls, host server operating systems, databases, and application systems. Tencent Cloud uses scanning tools to continuously detect deviations between the configurations of operating systems, database management systems, and virtual images and the established standards. For identified deviations, Tencent Cloud automatically generates security work orders and sends them to the responsible teams for timely remediation. Tencent Cloud's security team also conducts regular reviews of the security policies and parameter settings of network devices such as routers, firewalls, and network servers to ensure the effectiveness of these policies and parameters.

No.	Domain	Summary of Controls	Tencent Cloud's Response
9.07-9, 09, 9.11-9.12	Cyber Security Monitoring	9.07 A capital market entity must establish—	Customers should establish a security operation center or engage a managed security services provider to monitor cybersecurity incidents. Customers should also actively monitor cybersecurity incidents, detect abnormal activities, and collect and review system logs, conducting correlation analysis on multiple incidents recorded in the logs. Additionally, baseline indicators of the IT system should be monitored. Any anomalies or suspicious behaviors should be analyzed and reported immediately upon detection.
		(a) on a best effort basis, a security operation centre (SOC) or engage a managed security services (MSS) provider that has sufficient capabilities for pre-emptive surveillance and monitoring of its cyber events. The SOC implemented must be secured with proper access controls, skilled resources, and accommodated with disaster recovery capabilities and dashboard to oversee the overall network perimeter of the capital market entity;	The Cloud Security Center (CSC) aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Customers can also use Cloud Audit to record logs and continuously monitor account activity across Tencent Cloud infrastructure.
		(b) a process to collect, review and retain system logs to facilitate the cyber events monitoring operations of the capital market entity while ensuring the system log remains protected; and	Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Tencent Cloud also operates an internal network monitoring system to monitor and alert on network devices such as routers, firewalls, and servers, and uses a ticketing system to track and resolve identified security issues. Tencent Cloud has defined detailed operational security “red lines” and, leveraging years of experience in abnormal behavior monitoring, built a comprehensive rule base and automated auditing tools. These tools enable reliable detection of abnormal activities and automatically trigger real-time alerts.
		(c) a baseline indicator for each of the IT systems being monitored. Any anomalies or suspicious user behaviour detected against the baseline indicator must be analysed and escalated in a timely manner in accordance with the escalation and decision-making processes of the capital market entity.	
		9.08 A capital market entity must establish a monitoring and detection process to support continuous surveillance of any cyber event, which should include,	Tencent Cloud uses scanning tools to check the configurations of operating systems, database

No.	Domain	Summary of Controls	Tencent Cloud's Response
		among others, clearly defined escalation and decision-making processes to ensure any adverse effect of a cyber incident is properly managed.	management systems, network devices, and virtual images, continuously detecting deviations from the standard configurations defined in baseline files. Once a deviation is identified, the system automatically generates a security ticket and sends it to the responsible department for timely remediation.
		9.09 A capital market entity must proactively monitor any cyber event, detect any anomalous activity and conduct analysis on any detected event that may have material impact on the business or systems of the capital market entity.	For incident detection and response , Tencent Cloud has established a detailed incident management process and uses an internal security operations system to record security incidents. Detected incidents are analysed and classified based on nature, data sensitivity, and impact scope, and relevant personnel are promptly notified for follow-up.
		9.11 A capital market entity must perform correlation of multiple events registered on system logs to identify anomalous system activity or suspicious user behaviour patterns according to the baseline indicator.	
		9.12 If reasonably practicable, a capital market entity must apply advanced user behavioural analysis to detect sophisticated cyber events such as signature-less and file-less malware, as well as to identify anomalies at endpoints and network layers.	
9.13 、 9.14	Threat Detection	9.13 A capital market entity must regularly review its cyber threat analysis report that commensurate with its business model, risk appetite and technology dependency. The cyber threat analysis report must be communicated to its senior management. At the minimum, the report must	Customers should establish the capability of cybersecurity situation awareness, and collect, process and analyze the relevant cybersecurity information that may have an impact on their business and IT environment. To support customers in threat detection and analysis, Tencent Cloud provides the Threat Intelligence Center (TIX) , a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface

No.	Domain	Summary of Controls	Tencent Cloud's Response
		encompass the cyber threat trends and statistics, incidents grouping by type of attack, target and source of IP addresses. 9.14 A capital market entity must equip itself with the knowledge and understanding of the current and evolving cyber threats, new cyber attack techniques, analyse and determine the appropriate countermeasures.	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, 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.
9.15 、 9.16	Cyber Security Incident Response	9.15 A capital market entity must establish a cyber incident response capability to manage and minimise damage from cyber incidents, and to recover and learn from such incidents. The cyber incident response capability must encompass the following phases: (a) Preparation: A capital market entity must establish an effective governance process, reporting structure and a team to manage cyber incident and response plan in the event of a cyber incident that cause service disruption. A capital market entity must also clearly	Customers should establish procedures and processes for responding to and recovering from cybersecurity incidents, defining the relevant parties to be contacted and the communication contents during the incident. Analyze the root causes of the incident and take corrective measures, and draw lessons from the experience gained. To help customers detect and respond to incidents quickly, Tencent Cloud provides a one-stop security management platform—Cloud Security Center (CSC). Through its Asset Center, Risk Center, Alert Center, and advanced security management features, CSC enables customers to achieve a closed-loop security operation covering proactive threat detection, real-time incident response, and post-incident forensic analysis, thereby improving the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		define the roles and responsibilities of the team.	efficiency of security operations.
		(b) Detection and Analysis: A capital market entity must establish a detection process to handle detected cyber events, including disaster declaration and classification of the cyber incident based on the attack vectors. Different types of cyber incidents merit different response strategies.	For incident response and management, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up.
		(c) Containment, Eradication and Recovery: A capital market entity must establish a recovery process to mitigate any service disruption due to cyber-attack by prioritising the recovery based on the criticality of the systems and services within a capital market entity operating environment and to restore IT systems to its normal operation.	During the process of receiving, investigating, evaluating, handling and tracking information security incidents, the relevant responsible departments will maintain the relevant records of the received information security incidents and ensure the completeness and confidentiality of the records. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review.
		(d) Post Incident Review: A capital market entity must ensure that the recovery process carried out by the capital market entity event is well documented to support an effective post incident review. A report must be produced from the post incident review and presented to all relevant stakeholders.	Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type, frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence.
		9.16 A capital market entity must establish clearly defined communication plan including escalation and decision-making processes to ensure	In terms of communication and notification of the incident, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as

No.	Domain	Summary of Controls	Tencent Cloud's Response
		that any adverse effect of a cyber incident is properly managed and recovery action may be initiated quickly.	announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses. Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.
9.17-9.19	Cyber Security Incident Recovery	9.17 For the purposes stated in paragraph 9.15(c), a capital market entity must identify the critical systems and services within its operating environment that shall be recovered on a priority basis in order to provide an acceptable level of services during the downtime. 9.18 A capital market entity must determine the recovery time objective to return to its full service and operations. 9.19 A capital market entity must regularly review and update the cyber incident	Customers should set service recovery time objectives for each critical business service and formulate corresponding recovery strategies. Customers should determine the business recovery priorities, recovery strategies and resource allocation based on the criticality of business services and functions. After an operational disruption occurs, customers should review and improve the business continuity management measures, draw lessons from its own or other organizations' incidents, and enhance the level of business continuity preparedness. To support the Customer in meeting regulatory requirements, Tencent Cloud conducts business impact analysis for its cloud products and services in accordance with its internal business

No.	Domain	Summary of Controls	Tencent Cloud's Response
		management plan taking into account the information gathered from reputable cyber threat intelligence and lesson learned from cyber incidents.	continuity management policies. This analysis includes identifying critical products and services, mapping activities that support service delivery, assessing the impact of disruptions over time, establishing recovery priority timelines at the minimum acceptable level, identifying dependencies and supporting resources, and formulating appropriate response strategies based on the analysis results. To ensure continuous availability of Customer operations, Tencent Cloud performs business impact analysis for its cloud products and services, defines RTOs and Recovery Point Objectives (RPOs), and develops response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans are established for cloud products and critical processes. The relevant policies, plans, and contingency measures cover critical areas such as facilities, personnel, equipment, systems, and information data. Corresponding disaster recovery processes are established based on business priorities to ensure the disaster recovery system is complete, orderly, and executable. Tencent Cloud regularly conducts business continuity drills and tests based on these plans to ensure their feasibility. Tencent Cloud has established continuous improvement procedures and mechanisms that define corrective, preventive, and improvement actions after an incident occurs. Tencent Cloud analyzes the actual or potential causes of incidents or issues, evaluates the need for corrective and preventive measures, identifies improvement opportunities, and implements approved actions. For incidents that result in operational disruption, Tencent Cloud's quality management department organizes a post-incident review with the responsible teams, summarizes lessons learned, and issues an incident investigation report. The quality management department monitors the

No.	Domain	Summary of Controls	Tencent Cloud's Response
			implementation of subsequent improvements to prevent recurrence of similar incidents. Tencent Cloud conducts an annual assessment of the completeness, adequacy, and effectiveness of its business continuity management system and revises the system based on the assessment results. Tencent Cloud also reviews its business continuity plans annually and updates them as necessary. When significant changes occur in business functions or critical resources, Tencent Cloud reviews the scope of critical services and their component dependencies and promptly revises the business continuity plans.
9.20-9.25	Cyber Security Assessment	9.20 A capital market entity must establish a process to conduct regular assessment, and to identify potential vulnerabilities and cyber threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks. The process must, among others, outline the relevant control measures to mitigate any vulnerabilities and cyber threats in its operating environment. 9.21 A capital market entity must ensure its assessment is comprehensive, which comprise among others making an assessment of potential vulnerabilities relating to systems and technologies adopted including any third-party systems utilised by the capital market entity and business processes.	Customers should conduct regular vulnerability assessments and penetration tests to identify security vulnerabilities and evaluate their cybersecurity protection capabilities. Analyze the vulnerabilities discovered during the cybersecurity assessment, and classify them based on their severity to set clear repair deadlines. For penetration testing, Tencent Cloud offers the Penetration Testing Service (PTS) which fully simulates attack techniques and vulnerability exploitation methods commonly used by hackers. PTS uses controlled, non-destructive approaches to deeply probe the security of target systems, identify weaknesses in targets and network devices, and provide hardening recommendations to help customers improve system security. It also supports validation after vulnerability remediation. For vulnerability scanning, customers can use the Vulnerability Scanning Service (VSS) to detect risks in enterprise network assets. Leveraging Tencent's extensive security experience and threat intelligence, VSS maintains a comprehensive vulnerability rule base and provides professional detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		9.22 Where feasible, a capital market entity should regularly undertake a compromise assessment (CA) on its critical systems to prevent and detect any potential compromise of its security posture. 9.23 A capital market entity must conduct regular penetration testing exercise to imitate an experienced hacker attacking the production environment of the capital market entity, with the aim to obtain in-depth evaluation of its cyber defences. The scope and frequency of the exercise must commensurate with the capital market entity's risk exposure and should at a minimum be conducted annually. 9.24 A capital market entity must ensure the penetration testing exercise process is documented and performed by experienced and qualified professionals who are aware of the risk of undertaking such exercise and are able to limit the damage resulting from a successful break-in to a production environment. A capital market entity must obtain the approval of its senior management before finalisation of the test scope. 9.25 A capital market entity must establish a comprehensive remedial process to track, monitor and resolve vulnerabilities	scans, continuous risk alerts, and vulnerability detection for customer assets, assessing availability, security, and compliance. It also provides professional remediation advice to reduce security risks. VSS can integrate with other Tencent Cloud products such as Host Security and Web Application Firewall to achieve a closed-loop process from risk monitoring to risk mitigation. To support regulatory compliance, Tencent Cloud regularly schedules vulnerability scans for cloud environment assets and analyzes, categorizes, and remediates detected vulnerabilities. Tencent Cloud also conducts full-chain large-scale penetration tests to proactively identify and fix potential security risks and performs targeted penetration tests before new product launches or major changes. Penetration test results are communicated via security tickets to responsible departments for timely remediation or compensating controls. Tencent Cloud conducts red team vs. blue team adversarial exercises to simulate real-world cyberattacks. Tencent Cloud has also established an external vulnerability reporting platform and operates a Bug Bounty Program, inviting industry security experts to identify vulnerabilities and risks from a hacker's perspective, enabling timely remediation and maintaining Tencent Cloud's ecosystem security.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		identified from the cyber security assessments. The remedial process must include at a minimum: (a) severity level and classification of identified vulnerabilities; (b) turnaround time to remediate vulnerabilities according to its severity level; and (c) risk assessment and mitigation plans to manage exceptions (i.e. for vulnerabilities which the capital market entity is unable to remediate timely) with approval from senior management.	
9.26-9.28	Cyber Simulation Exercise	9.26 A capital market entity must carry out a cyber simulation exercise which commensurate with the level of risk appetite of the capital market entity and its reliance on technology to test the effectiveness of its cyber incident response and recovery, including its communication plan based on current and emerging cyber threat scenarios. A capital market entity must determine the objectives, scope and conditions of engagement for the cyber simulation exercise before the initiation of the exercise. It must ensure the simulation exercise is conducted with involvement	Customers should conduct regular cyber simulation exercises to verify their response capabilities and the effectiveness of communication in dealing with cyber threats. Additionally, customers should conduct adversarial simulation attack drills on the infrastructure of the third-party service providers they have entrusted, in order to identify the cyber defense and response capabilities of the third-party service providers. Tencent Cloud's internal business units periodically conduct scenario-based training and drills for security incident response plans. Tencent Cloud also provides ongoing technical training for its security teams based on evolving technologies and threat landscapes, ensuring staff understand and comply with the latest security standards and best practices and can respond quickly and effectively to security incidents. Tencent Cloud regularly conducts red team vs.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		from key stakeholders.	blue team exercises simulating real-world cyberattacks to test and validate its ability to respond to network attacks.
		9.27 To ensure the capital market entity is prepared to respond to cyber incidents detected, at a minimum, the capital market entity must—	In response to customers' needs for cybersecurity drills on cloud-based information assets, Tencent Cloud will actively evaluate and provide technical support to collaborate with customers in completing the drill implementation.
		(a) identify scenarios of cyber risk that it is most likely to be exposed to;	
		(b) consider incidents in the capital market and the broader financial services industry;	
		(c) assess the likely impact of these incidents to the capital market entity; and	
		(d) identify appropriate response plan and communication strategies that should be undertaken.	
		9.28 Where feasible, a capital market entity should perform an adversarial attack simulation exercise on the infrastructure hosted with third-party service providers to identify potential vulnerabilities of its cyber defence and response plan against rampant cyber threats.	

11.6 Guiding Principles Relating to The Adoption of Artificial Intelligence (AI) and Machine Learning (ML)

Appendix 3 of the [Guidelines on Technology Risk Management](#) specifies four principles for capital market entities that adopt artificial intelligence (AI) and machine learning (ML), namely: (i) Accountability; (ii) Transparency and Explainability; (iii) Fairness and Non-Discrimination; and (iv) Practical Accuracy and Reliability. This appendix sets out regulatory requirements for the application of AI and ML technologies, suggesting that a capital market entity should establish and implement a robust and sound governance framework and process to oversee the development and

use of its AI and ML; A capital market entity should be able to explain what went into making a specific decision by the AI and ML, to ensure that users or groups of users are not systematically disadvantaged or discriminated; A capital market entity should ensure that data and models used for AI and ML driven decisions are regularly reviewed and validated to guard against the use of biased data or algorithms; and ensure privacy, data protection and security in AI systems by employing data governance and management, throughout the data lifecycle; and ensure robust security and resilience of its AI systems through, among others, the implementation of appropriate controls and security measures.

When complying with this guideline, Tencent Cloud, as a service provider of AI products, may be involved in certain activities related to regulatory requirements. This section explains how Tencent Cloud helps capital market entities meet relevant requirements under Appendix 3 of the guideline.

Tencent Cloud regards responsible AI development as one of its long-term strategic priorities. While driving business growth, we are committed to embedding ethics and security into AI technology development and application to foster responsible innovation. We place great importance on addressing security challenges posed by AI, actively aligning with global governance trends, and continuously improving AI governance to mitigate potential risks. In compliance with applicable laws and regulations, we prioritize data quality, security, compliance, and ethical considerations throughout the AI lifecycle, conducting risk assessments and implementing a series of risk management measures. Tencent Cloud invests heavily in areas such as security classification systems, adversarial defence, detection of covert harmful content, training data desensitization, and embedding social ethics, to ensure safe AI operations and address emerging risks in data security, model security, and AI ethics.

In data governance, Tencent Cloud establishes and enforces data security policies to comprehensively manage AI data processing across its full lifecycle. We integrate security and compliance requirements into the entire AI development process, rigorously review and select highly trusted data sources, and apply advanced algorithms for deep data cleansing and secure filtering. These measures ensure AI data remains protected and legally used, building a strong defence for user privacy and data security. Additionally, Tencent Cloud's AI security team has conducted large-scale internal security tests involving thousands of participants to proactively identify and mitigate AI security risks in areas such as content safety, privacy protection, and model security.

In algorithm governance, Tencent Cloud continuously evaluates and adjusts AI algorithm security, regularly identifying and fixing potential vulnerabilities, testing and strengthening model resilience against attacks, optimizing performance, and reducing bias. We have also established cross-functional security review mechanisms to ensure models meet both business needs and security standards in technical implementation and data usage.

In operational governance, Tencent Cloud monitors, prevents, and responds to risks on an ongoing basis, implementing multi-layered security protections to ensure safe and accurate model outputs. We apply content tagging technologies to track risky content and continuously enhance model security, reinforcing our commitment to user and societal responsibility. Tencent Cloud also conducts regular disaster recovery drills simulating real-world scenarios, including adversarial attacks and large-scale failures, to comprehensively test system resilience, response speed, and recovery capabilities, ensuring rapid business restoration in emergencies.

Tencent Cloud offers a wide range of AI and machine learning products, including:

- **AI Foundation Products**

- [Face Recognition](#): Accurate, real-time face detection, analysis, and large-scale face search services.
- [Automatic Speech Recognition \(ASR\)](#): Highly cost-effective speech recognition with exceptional accuracy for multiple scenarios.
- [Text-to-Speech \(TTS\)](#): Professional, intelligent, and efficient voice synthesis services.
- [Tencent Machine Translation \(TMT\)](#): High-quality, efficient translation supporting over ten languages.
- [Optical Character Recognition \(OCR\)](#): Fast, accurate text recognition across diverse image scenarios.
- [Image Creation](#): AI-powered image generation and processing tools for creative expression.
- [Face Fusion](#): Advanced facial feature blending for creative applications.

- **AI Application Products**

- [Face Recognition](#): Secure and efficient identity verification using facial recognition.
- [Tencent Cloud AI Digital Human](#): Next-generation multimodal interaction system for creating intelligent, interactive digital avatars.

- **AI Platform Products**

- [Tencent Cloud TI Platform](#): A one-stop machine learning platform offering end-to-end support—from data preprocessing and model training to deployment—featuring rich algorithm components and multi-framework compatibility. For financial institutions, TI Platform enables predictive modelling for personalized product recommendations, improving efficiency and customer experience.

- **Tencent Large Model Products**

- [Tencent Cloud Agent Development Platform](#): Provides advanced capabilities such as OCR, LLM+RAG, and MLLM for intelligent document parsing and knowledge extraction. The platform supports multimodal knowledge integration, precise Q&A, and iterative optimization through configurable tools for testing, correction, publishing, and feedback enhancement.

12

How Tencent Cloud Meets and Assists Customers to Meet the SC Requirements of Guiding Principles on Business Continuity

To enhance the awareness on the importance of having an effective business continuity arrangement, the Securities Commission Malaysia released the [Guiding Principles on Business continuity](#) in 2019. It serves as a guidance on the Securities Commission Malaysia's expectations on business continuity. The SC, with its supervisory responsibility over capital market entities, requires each capital market entity to have business continuity management arrangements as part of ensuring systemic resiliency of the Malaysian capital market. The overall intended outcomes of the principles are to ensure timely continuation of critical services and the fulfilment of business obligations in the event of disruptions and ultimately with the objectives to mitigate or manage any possible wider systemic risk³ implications to the Malaysian capital market. The requirements mainly focus on areas such as Major operational disruptions, Recovery objectives and strategies, Communications, Testing and Training and Maintenance and Review.

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 and extracts the control requirements relevant to cloud service providers as outlined in Guiding Principles on Business continuity, and explains how Tencent Cloud, as a cloud service provider, assists capital market entities in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.08	Risk Identification	3.08 The SC recommends that capital market entities should consider and monitor the following: (a) Financial and non-financial risks potentially arising from internal and external factors; (b) Risks that may arise from the interdependencies of critical business functions as well as the extent to which they depend on other parties; (c) Concentration risks arising from centralisation of critical and support functions; and (d) Risks of outsourcing its critical business functions to third-party service providers.	Customers should identify and detect potential risks both internally and externally, including dependency risks, concentration risks, and outsourcing risks, etc. Tencent Cloud conducts risk assessments for cloud products and services based on its internal business continuity management regulations. The main contents of risk assessment include: Identify business continuity-related resources and their values, identify threats to business continuity resources, identify the vulnerability of resources, comprehensively analyze the possibility of various threats and quantitatively or qualitatively describe the impact, and objectively evaluate the effectiveness of existing risk prevention and control measures.

No.	Domain	Summary of Controls	Tencent Cloud's Response
3.10	Risk Assessment	3.10 The entity may choose to assess the impacts of operational disruptions on its critical business functions via business impact analysis and identify the critical business functions or operations that are necessary to be prioritised in its recovery strategies.	Customers should conduct a risk assessment and business impact analysis to evaluate the impact of operational disruptions on critical business functions, in order to clearly identify the critical business functions or operations that are necessary to be prioritised in its recovery strategies. 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.
3.11	Infrastructure	3.11 When assessing the probability of a disruption, the entity is encouraged to take into consideration the geographical locations of all facilities, their susceptibility to threats, and the proximity to key infrastructure. This is followed by gauging and determining the severity of the disruption. The entity can then take appropriate mitigating measures to manage the disruptions and ensure continuity and resumption of its critical business functions and business operations as a whole.	When assessing the probability of a disruption, customers should take into account the geographical location of all facilities, their susceptibility to threats, and the proximity of critical infrastructure, in order to determine the severity of the interruption and take appropriate mitigation measures. 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.
3.13	Allocate Resources	3.13 With clear risk management objectives, the	Customers should determine the priority of business recovery, recovery strategies, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		entity may align both its priorities and resources. As resources are generally scarce, the entity should effectively allocate necessary resources in order to plan for the continuity and resumption of its business activities and operations.	resource allocation based on the criticality of business services and functions. To support the Customer in meeting regulatory requirements, Tencent Cloud conducts business impact analysis for its cloud products and services in accordance with its internal business continuity management policies. This analysis includes identifying critical products and services, mapping activities that support service delivery, assessing the impact of disruptions over time, establishing recovery priority timelines at the minimum acceptable level, identifying dependencies and supporting resources, and formulating appropriate response strategies based on the analysis results.
3.15 、 3.16	Recovery objectives and strategies	3.15 Capital market entities are encouraged to develop recovery objectives and strategies that reflect the risk they represent to the operation. Recovery objectives and strategies may also be developed for specific business functions, which should be established in consultation with, or by, the respective business unit. Ultimately, the board of directors and senior management are responsible for the recovery objectives and strategies. 3.16 Recovery objectives and strategies should include identification of recovery levels and recovery time objectives for specific business lines. This aims to give assurance on the level of resilience and recovery timeframe during an	Customers should formulate recovery objectives and strategies based on the results of risk assessment and business impact analysis, and identify the recovery levels and recovery time objectives for each business line. To ensure continuous availability of Customer operations, Tencent Cloud performs business impact analysis for its cloud products and services, defines RTOs and Recovery Point Objectives (RPOs), and develops response strategies and business continuity plans based on the analysis results. Detailed disaster recovery plans are established for cloud products and critical processes, covering facilities, personnel, equipment, systems, information and data, and business priorities.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		operational disruption. This information may serve as a benchmark when testing adequacy of business recovery approaches.	
3.17	Alternate site	3.17 The SC encourages capital market entities to have access to at least one or more recovery sites in the event where the primary site is inaccessible. Some of the factors that may be considered for recovery arrangements include– (a) geographical location of the recovery site and its proximity to the primary site; (b) adequacy of current data, equipment and system; and (c) availability of sufficient staff, in terms of numbers and expertise, to recover critical operations and services.	Customers should ensure that there is at least one or more recovery sites available when the main site is unavailable. When selecting alternate sites, customers should consider the distance between the two sites, the sufficiency of data, equipment and systems, as well as the number and professionalism of the personnel. To assist customers in meeting regulatory requirements, 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. In 2026, Tencent Cloud launched three data centers in Malaysia, offering a range of cloud computing services including cloud servers, cloud databases, and CDN. Customers can flexibly deploy data, systems and its backup 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 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
			levels. All visitors and staff must undergo identity verification, personal item checks, and item registration before entering the data center.
3.18 、 3.19	Communications	3.18 Successful deployment and execution of a business continuity framework is highly dependent on co-ordinated, coherent, timely and effective communications within the entity and with its relevant external stakeholders in order to ensure consistent messaging and minimise reputational risks during major operational disruptions. 3.19 The SC recommends that capital market entities' business continuity framework to include comprehensive escalation and communication procedures as well as contact information of all stakeholders, including employees, counterparties, clients, service providers, building management, regulatory authorities, government agencies, emergency services and media. In addition, entities are encouraged to take into account alternative methods of communication in the case of interruptions of primary method of communication.	Customers should formulate a communication strategy and plan, which should include a list of internal and external contacts, key communication information, communication channels, and communication protocols, etc. To assist Customers in fulfilling communication and notification obligations, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses. Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.
3.24-3.27	Testing	3.24 Testing for critical business functions should be carried out at least annually. Senior management and employees who are involved are encouraged to participate in these exercises to promote awareness, familiarity and understanding of their roles and responsibilities within the scope of the approach towards business continuity. 3.25 Testing objectives may include the integration of core components of the approach adopted for business continuity as well as incorporating various interdependencies within and outside of the entity's business operations. In conducting a testing exercise, the SC recommends considering different levels of complexity, degree of employee or service provider participation, types of critical functions as well as different physical locations. 3.26 At the end of each testing exercise, the entity is encouraged to prepare a formal documentation of the post-mortem reviews of the testing programme. Testing results should be assessed to incorporate the necessary changes or remedial actions	Customers should test for critical business functions should be carried out at least annually. The test scope should cover the parts executed by the key service providers, ensuring that the key service providers participate in the tests. In addition, when designing and implementing the tests, customers should formulate a test plan, keep formal test documents, compile post-test analysis reports, identify problems and specify rectification plans, and report the test results to the management. Customers can leverage the Tencent Cloud Smart Advisor (TSA) service to assist with planning and executing business continuity tests. This service is a cloud governance platform that integrates multiple ITOM vertical applications and draws on Tencent Cloud's extensive operational expertise. Through risk inspections, fault drills, and other governance measures, Cloud Advisor optimizes cloud infrastructure. For stress testing, Tencent Cloud provides Performance Testing Service (PTS), which simulates real business scenarios with massive user traffic to comprehensively validate system availability and stability. PTS supports multi-region traffic generation with millions of concurrent requests and offers features such as traffic recording, scenario orchestration, traffic customization, and advanced script configuration. These capabilities enable Customers to quickly define stress test scenarios based on business models, accurately replicate large-scale application access patterns, and identify potential performance issues in advance.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		into the existing approach for business continuity, while the overall programme is evaluated for its effectiveness in achieving the testing objective and incorporating appropriate testing coverage. 3.27 Documentation relating to the testing programme and results should be prepared for senior management to sign-off and to be reported to Board of Directors for endorsement. These documentations should be made available upon the SC's request.	To support regulatory compliance, Tencent Cloud regularly conducts drills and tests for emergency response and disaster recovery internally. Tencent Cloud performs risk assessments on the drill plans to avoid any negative impact on services due to the drills. Disaster recovery drills typically simulate real-world disaster scenarios, including attack-defense exercises and large-scale failures, to thoroughly assess system resilience, response speed, and recovery capability. After each drill, relevant departments prepare a detailed drill report, which is archived along with the drill plan. The report generally includes the drill objectives and scope, execution plan, participants, preparatory work, key processes and timelines, identified issues, corrective measures and implementation plans, and conclusions. For issues identified during drills, Tencent Cloud implements corrective actions and promptly updates corresponding emergency plans. The audit department monitors the implementation of these corrective actions to ensure effectiveness.
3.28	Training	3.28 Capital market entities are encouraged to provide training to key business continuity coordinators to ensure adequate skillsets and competencies in managing or organising business continuity testing as well as to encourage awareness.	Customers should provide training to the key business continuity coordinators to ensure that they possess sufficient professional skills to organize and conduct business continuity tests. Tencent Cloud conducts regular emergency drills related to security incident response and provides ongoing technical training to security team members. These training programs ensure that employees understand and comply with the latest security policies and procedures and are familiar with current information security standards and best practices.
3.29-3.31	Maintenance and Review	3.29 Maintenance and reviews may not be limited to only after testing or restricted to a scheduled basis. Any significant changes in terms of technological, procedural	Customers should incorporate the business continuity policies and plans into their daily business operations on a regular basis, and conduct regular reviews and updates of the documents. The business continuity framework is independently reviewed by the internal and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		updates as well as changes in the roles and responsibilities of employees should be reflected as and when it occurs. 3.30 A capital market entity may incorporate maintenance and review as part of their day-to-day business operations. A designated team and/or officer should be in charge of maintaining relevant documentations. A copy of the entity's framework for business continuity should be made available to the SC upon request or during the SC's supervisory activities. 3.31 Amendments or updates should be acknowledged and signed-off by the Board and senior management. Independent review of the business continuity framework may be performed by the internal or external audit functions of the entity.	external audit functions. To support regulatory compliance, Tencent Cloud conducts an annual assessment of the completeness, adequacy, and effectiveness of its business continuity management system and revises the system based on the assessment results. Tencent Cloud also reviews its business continuity plans annually and updates them as necessary. When significant changes occur in business functions or critical resources, Tencent Cloud reviews the scope of critical services and their component dependencies and promptly revises the business continuity plans.

13

Conclusion

Tencent Cloud is the cloud computing brand developed by Tencent Group, built upon years of technological expertise and security practices. Tencent Cloud is committed to continuously providing secure, reliable, and intelligent cloud services, empowering more enterprises to embrace digital transformation efficiently and advance securely.

This guide is based on key regulatory requirements issued by the Bank Negara Malaysia and the Securities Commission Malaysia 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 Malaysia's compliance standards while achieving efficient digital upgrades and innovative business development.

This guide is for reference only. Customers are advised to apply the information herein based on their specific circumstances to ensure regulatory compliance when using Tencent Cloud services.

14

Version History

Date	Version	Detail
April 2026	V1.0	Initial Release