Tencent Cloud

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

April 2026

CONTENTS

01 Overview

The Insurance Authority (IA) is committed to regulating and supervising the insurance industry to promote its sound development and overall stability. To achieve this, the IA has issued a series of regulatory manuals, guidelines, and circulars, implementing effective supervisory strategies to foster the sustainable development of the insurance market.

With the growing adoption of digital and online channels in business operations, particularly in the promotion of insurance products and customer services—the IA strives to create a regulatory environment that supports business expansion while embracing technological innovation.

In this context, the IA has introduced specific regulatory requirements for authorized insurers in areas such as cybersecurity, conducting insurance activities via the Internet, and outsourcing arrangements. These measures aim to ensure that authorized insurers[1] can leverage modern information technologies to enhance operational efficiency and service quality, while effectively managing potential risks and safeguarding customer interests.

Tencent Cloud closely monitors regulatory developments and publications from the IA and is committed to supporting Hong Kong insurance institutions in meeting IA's regulatory requirements. This document outlines how Tencent Cloud assists customers in complying with key IA guidelines and circulars of relevance to authorized insurers.

- GL20 Guideline on Cybersecurity
- GL14 Guideline on Outsourcing
- GL8 Guideline on the Use of Internet for Insurance Activities

[1] Authorized insurer means an insurer authorized to carry on insurance business in or from Hong Kong, but excludes Lloyd's, captive insurers, special purpose insurers, marine mutual insurers, and any insurer that has ceased underwriting or accepting new insurance business in Hong Kong and is in the process of discharging its insurance liabilities.

02

Tencent Cloud Security and Privacy Compliance

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

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

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

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

2.1 Global Compliance

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

2.2 ISO/IEC Certification

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

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

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

2.3 Regional and Industry Compliance

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

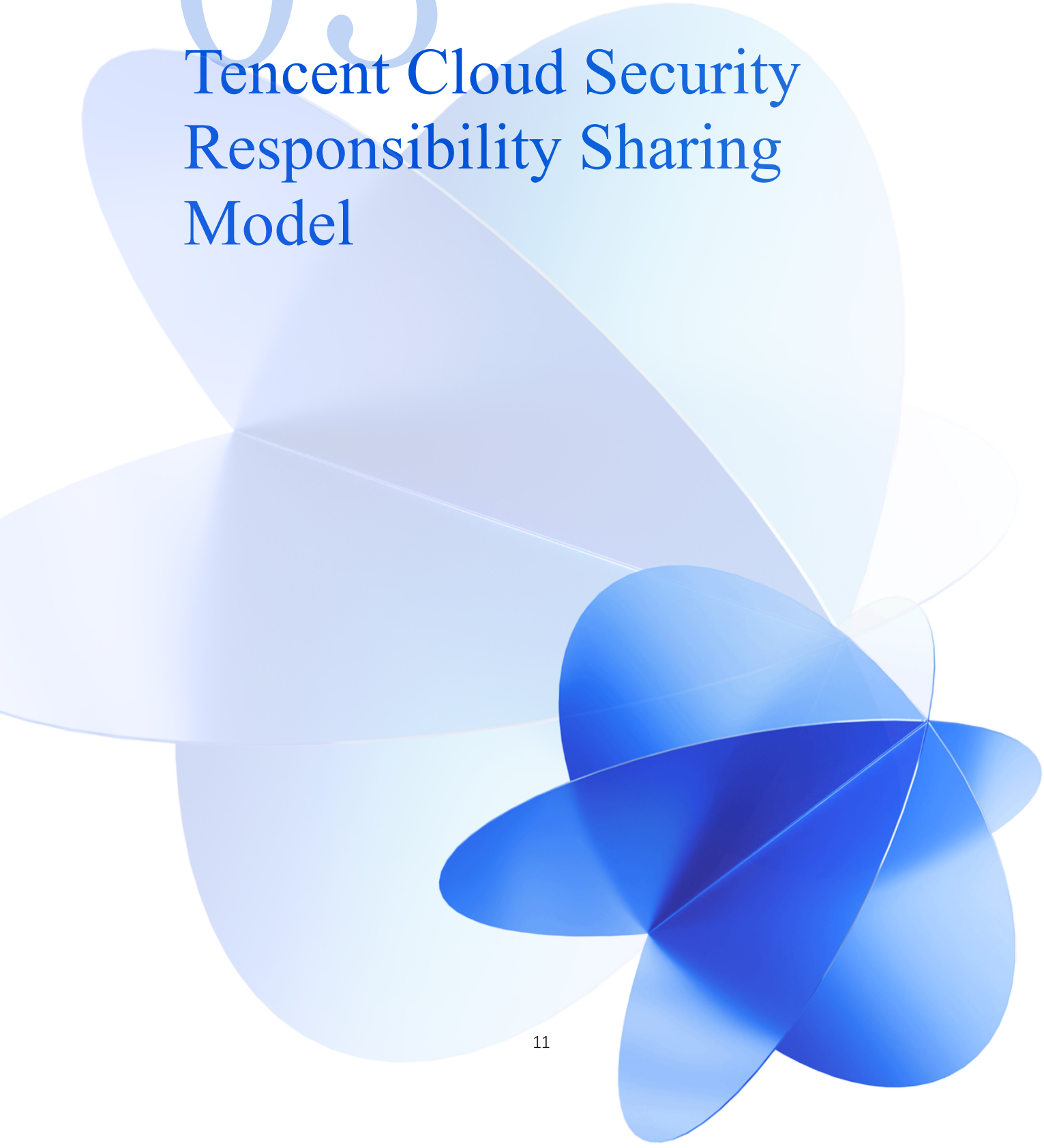
	design and operational effectiveness of controls in three areas: entity-level controls, general IT controls, and service controls. Tencent Cloud has obtained OSPAR attestation for multiple products and services in the Singapore region, demonstrating that its security capabilities meet the stringent requirements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

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

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

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

03 Tencent Cloud Security Responsibility Sharing Model



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

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

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

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

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

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

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

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

04 Tencent Cloud Global Infrastructure

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

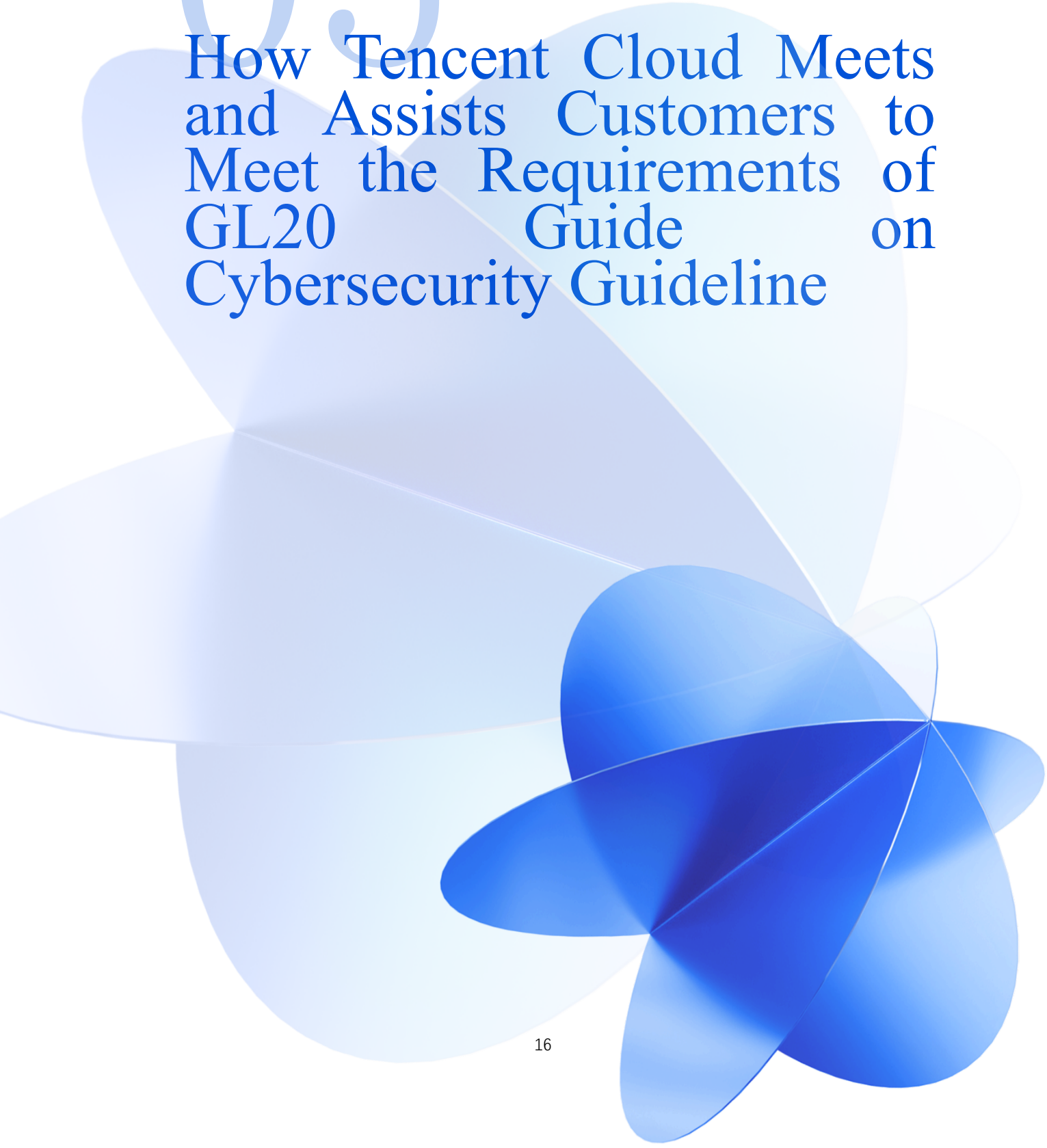
- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically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

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

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

05

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of GL20 Guide on Cybersecurity Guideline



GL20 Guide on Cybersecurity Guideline aims to define the minimum standards authorized insurers must meet in cybersecurity, establishing robust defensive measures to protect business data and the personal information of existing or potential policyholders, while ensuring business continuity. The requirements primarily focus on areas such as cybersecurity strategy and framework, risk identification, assessment and control, continuous monitoring, and incident response and recovery.

To assess whether authorized insurers' cybersecurity measures are adequate and effective, the Insurance Authority provides a Cyber Resilience Assessment Framework in the appendix. This framework helps insurers implement their cybersecurity framework effectively according to prescribed control principles and evaluate the inherent risk and maturity of their cybersecurity measures. The control principles are distributed across seven domains: Governance, Identification, Protection, Detection, Response and Recovery, Situational Awareness, and Third-Party Risk Management. The insurer's overall inherent risk level determines the required control principal level (Basic, Intermediate, or Advanced). The Cyber Resilience Assessment Framework aligns closely with the core content of the Cyber Resilience Assessment Framework (C-RAF) introduced by Hong Kong Monetary Authority (HKMA) in 2016 for authorized institutions. However, it is worth noting that the GL20 framework simplifies certain control principles compared to C-RAF.

As a cloud service provider, Tencent Cloud supports compliance and assists customers in meeting the relevant control principles outlined in the C-RAF 2.0 maturity assessment matrix. Authorized insurers may refer to the Tencent Cloud User Guide to C-RAF2.0 for guidance on relevant domains and requirements.

In this section, Tencent Cloud summarizes the control requirements in the GL20 Guideline on Cybersecurity that relate to cloud service providers and explains how Tencent Cloud helps authorized insurers comply with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.1-5.4	Cybersecurity strategy and framework	5.1 Authorized insurers should establish and maintain a cybersecurity strategy and framework tailored to mitigate relevant cyber risks that are commensurate with the nature, size and complexity of their business. The cybersecurity strategy and framework should be endorsed by the Board of the insurer. 5.2 Insurers, when establishing the cybersecurity strategy and framework, may make reference to or benchmark with the technology as well as the best available and practicable quality assurance standards,	Customers should establish a cybersecurity strategy and framework that aligns with their business nature, scale, and risk profile, and regularly review and update it. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, comprising an overarching security strategy, organizational structure, and management system. This framework effectively supports secure cloud platform operations and risk management, guiding daily work and management processes across all departments. Tencent Cloud reviews its information security policies annually to ensure that control objectives, procedures, and measures comply with relevant security standards, policies, and legal requirements, guaranteeing adequacy and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		taking into account of their business nature, size, complexity and risk profile. 5.3 The cybersecurity framework should clearly define the insurer's cybersecurity objectives, as well as the requirements for competency of relevant personnel or system users. It should include well-defined processes and technology necessary for managing cyber risks and timely communication of the strategy with all users. 5.4 Insurers should review and update regularly their cybersecurity strategy to ensure that the strategy remains relevant when there is significant change in their mode of business operation or in the external business environment (including external cyber risk landscape).	effectiveness. Employees can access these policies through internal platforms. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, CSA STAR, NIST CSF, and SOC, demonstrating that its security management and personal data protection practices meet recognized standards and industry best practices. Tencent Cloud also undergoes annual audits by independent professional third-party organizations.
7.1-7.2	Risk identification, assessment and control	7.1 Insurers should identify business functions, activities, products and services and maintaining a current inventory or mapping of its information assets and system configurations, including interconnections and dependencies with other internal and external systems; and prioritizing their relative importance 7.2 Insurers should regularly review and assess if changes to cyber risk mitigation processes are necessary when significant	Customers should establish a network risk management plan, conduct regular risk identification and assessment, and review their cybersecurity risk response processes. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an internal Information Security Risk Management Program that clearly defines and guides the entire risk management process, including risk identification, risk analysis, development of risk treatment plans, and risk tracking and monitoring. Tencent Cloud conducts risk assessment periodically, referencing sources such as industry security incident reports, Tencent Cloud's operational experience, and professional risk

No.	Domain	Summary of Controls	Tencent Cloud's Response
		changes to organizational and operational structure and systems take place.	databases to identify risks within its products and service processes. The assessment evaluates asset value, likelihood of risk scenarios, and potential impact to determine risk levels. Based on the analysis, Tencent Cloud develops response strategies and mitigation measures to reduce risks to an acceptable level. For each identified risk, Tencent Cloud assesses its likelihood and impact, assigns a risk level, and takes appropriate follow-up actions, documenting all results. Tencent Cloud continuously monitors risk treatment progress, evaluates residual risks, and ensures responsible parties manage risks in accordance with risk management requirements. Additionally, Tencent Cloud maintains and updates its risk assessment methodology and risk register based on industry trends and internal management practices.
8.1、8.2	Continuous monitoring	8.1 Insurers should establish systematic monitoring processes for early detection of cybersecurity incidents; regularly evaluate the effectiveness of internal control procedures; and update the risk appetite and tolerance limit as appropriate. 8.2 Insurers should establish an effective monitoring measures including, among others, network monitoring, testing, internal audit and external audit.	Customers should establish systematic cybersecurity monitoring to detect security incidents at an early stage through network monitoring, security testing, and internal and external audits. Through the **Tencent Cloud's Observability Platform (TCOP)**, customers can achieve real-time monitoring, analysis, and alerting for cloud products and resources. TCOP collects monitoring metrics reported by cloud servers, cloud databases, and other products, as well as user-defined metrics, and displays them through visual dashboards. This helps customers track resource utilization, application performance, and the operational status of cloud products in real time. TCOP also supports setting alerts for specific metrics and notifies customers promptly of business anomalies via message push based on configured alert rules. To assist customers in meeting regulatory requirements, Tencent Cloud has implemented an internal network monitoring system to monitor network devices and issue alerts, with identified

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security issues tracked and resolved through a ticketing system. Tencent Cloud regularly reviews the security policies and parameter configurations of network devices such as routers, firewalls, and servers to ensure their effectiveness.
8.3	Access Control	8.3 As part of the monitoring process, insurers should manage the identities and credentials for physical and remote access to information assets. They should recognize signs of a potential cyber risk, or monitor if an actual breach has taken place in their systems.	Customers should manage identities and credentials required to access information assets and implement monitoring measures to identify potential risks and review any violations. Customers can use **Cloud Access Management (CAM)** to assign resource permissions to sub-users through tags and other methods, enabling fine-grained access control for cloud resources. CAM also supports viewing and tracking employee operation records through **CloudAudit** .In addition, Tencent Cloud provides **Bastion Host (BH)**, which enables granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users have only the minimum privileges necessary to access assets and perform tasks. Bastion Host also supports operation auditing, recording and analysing user activity logs to ensure effective traceability of security incidents. Internally, Tencent Cloud has established authorization policies and a permission segregation matrix for access control. Tencent Cloud uses a Zero Trust security management system to authenticate employees, requiring two-factor authentication before accessing internal resources. Tencent Cloud monitors employee account login status in real time, and if any abnormal login activity is detected, the security system immediately contacts the account owner for verification and resolution, while recording the incident in detail. Tencent Cloud's production environment is fully integrated with Bastion Host, which centrally manages administrator account permissions for

No.	Domain	Summary of Controls	Tencent Cloud's Response
			backend system components. Internal operations personnel must obtain authorization approval before accessing Bastion Host (BH), and only designated Tencent Cloud staff are permitted to log in, which requires two-factor authentication. All operational records are stored centrally on a logging platform and are regularly reviewed by Tencent Cloud's internal audit team.
8.4	Cybersecurity Testing	8.4 Insurers should test all elements of their cybersecurity framework to determine their overall effectiveness at least on an annual basis. Insurers can use one or a combination of the latest available methodologies and practices, for example vulnerability assessment, scenario-based testing and penetration test.	Customers should conduct at least one cybersecurity-related test annually to evaluate the effectiveness of their security measures. Testing methods include, but are not limited to, vulnerability scanning and penetration testing. Tencent Cloud's **Vulnerability Scanning Service (VSS)** leverages years of accumulated security expertise and threat intelligence to maintain a comprehensive vulnerability rule base and provides professional, efficient detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS performs regular security scans, continuous risk alerts, and vulnerability detection on customer assets, assessing availability, security, and compliance, and offers professional remediation recommendations to reduce security risks. **Penetration Testing Service (PTS)** simulates attack techniques and vulnerability exploitation methods used by hackers in a controlled, non-destructive manner to deeply probe the security of target systems, identify weaknesses in targets and network devices, and provide hardening recommendations to help customers enhance system security. PTS can also be integrated into customers' product development, application launch, and security self-assessment plans. To support regulatory compliance, Tencent Cloud has established an internal mechanism for regular vulnerability scanning and penetration testing. Internal vulnerability scans typically include web vulnerabilities, component vulnerabilities, and configuration checks, with automated tasks generated by scanning systems to identify and

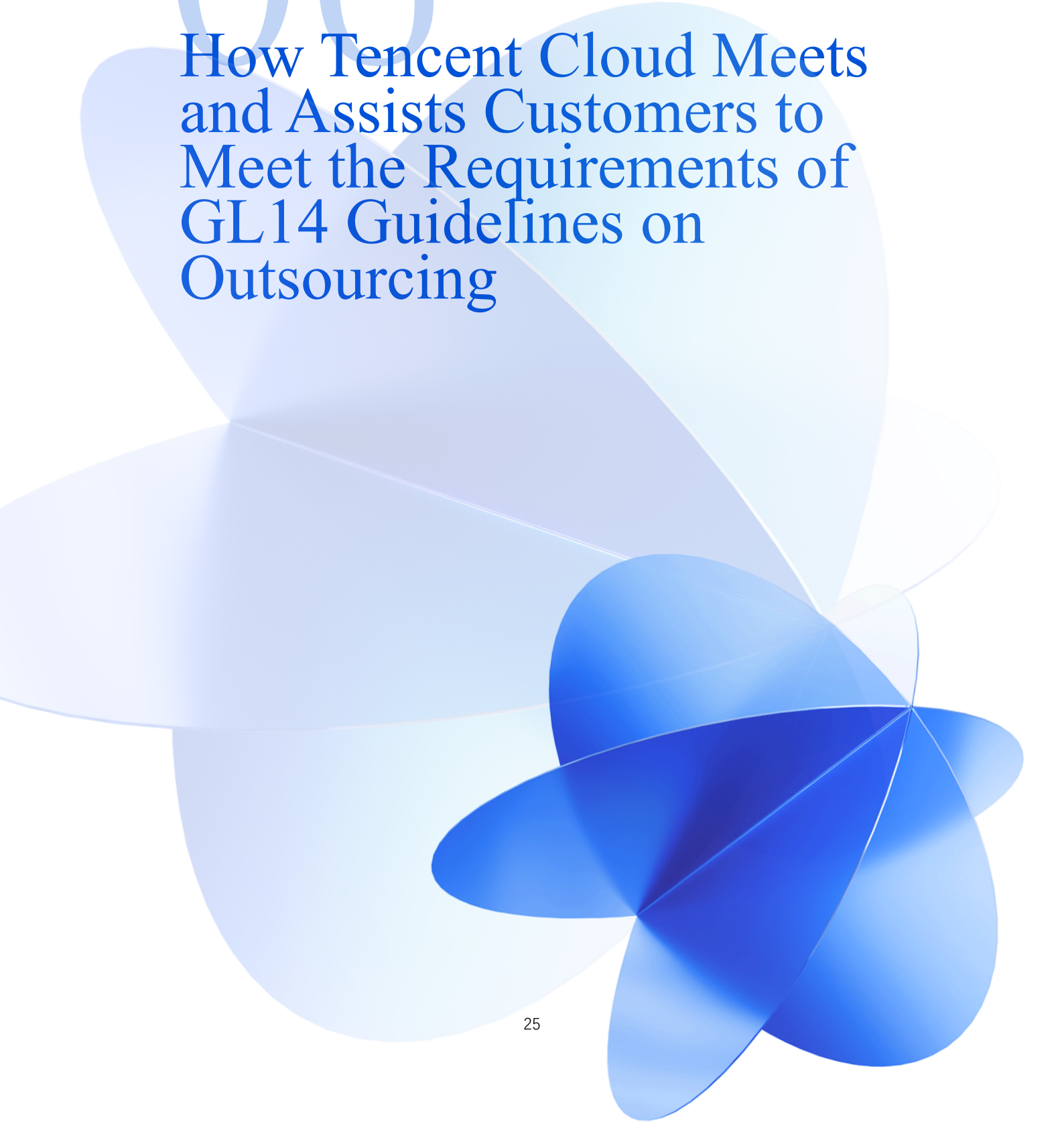
No.	Domain	Summary of Controls	Tencent Cloud's Response
			remediate vulnerabilities in cloud environments. For penetration testing, Tencent Cloud's security team conducts large-scale end-to-end tests periodically and targeted tests before new product launches or major changes. Test results are communicated via security tickets to responsible departments for timely remediation or compensatory controls, ensuring that exploitable vulnerabilities are properly addressed. Tencent Cloud regularly conducts red-blue team 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 fixes and maintaining ecosystem security. Tencent Cloud's security team continuously monitors and evaluates internal security risks to ensure the effectiveness and reliability of its Information Security Management System. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture in compliance with applicable laws, regulations, and security standards.
9.1-9.5	Response and recovery	9.1 Insurers should develop a cybersecurity incident response plan, which covers scenarios of cybersecurity incidents and corresponding contingency strategies to maintain and restore critical functions and essential activities in such scenarios. This should also include criteria for the escalation of the response and recovery activities to the Board or its designated management team. 9.2 In case of a cybersecurity incident, insurers should assess	Customers should establish an incident response mechanism that covers various cybersecurity scenarios, clearly defining processes for incident assessment, handling, notification, reporting, and post-incident review, and conduct at least one emergency drill annually. Cloud Security Center (CSC) is a one-stop security management platform that provides asset management, risk monitoring, alerting, and advanced security management capabilities, enabling customers to achieve a closed-loop security operation process encompassing proactive threat detection, real-time incident response, and post-incident analysis. To support customers in rapid incident response

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the nature, scope and impact of the incident and take all immediate practicable steps to contain the incident and mitigate its impact. 9.3 Insurers should notify internal stakeholders, and where applicable, external stakeholders and consider joint incident response actions, if necessary. In this regard, insurers should perform incident response drill at least on a yearly basis. 9.4 Upon the detection of a relevant incident, the insurer should report the incident with the related information to the IA as soon as practicable, and in any event no later than 72 hours from detection. 9.5 Once stable operations are resumed, insurers should identify and mitigate all vulnerabilities that were exploited, and remediate the identified vulnerabilities to prevent similar incidents as part of their recovery process from the relevant incident.	and handling, Tencent Cloud has developed an Information Security Incident Management Standard, establishing reporting, response, and handling mechanisms and related workflows. Tencent Cloud has formulated cybersecurity contingency plans for common scenarios such as network attacks, malware, data security breaches, equipment failures, and disaster events, and conducts regular emergency drills to ensure timeliness and feasibility. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyses and classifies them based on factors such as nature, data sensitivity, and impact scope, promptly notifying responsible personnel for follow-up. For incidents that may affect customers, Tencent Cloud, after internal review, communicates the handling and analysis results through appropriate channels and provides technical support to help customers implement remedial measures and minimize losses. Tencent Cloud has established a periodic incident analysis mechanism, conducting multi-dimensional reviews of incidents (type, frequency, impact scope, and severity) and implementing preventive measures based on root cause analysis to avoid recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a detailed analysis report for management. If a customer needs to report a cybersecurity incident to the Insurance Authority, Tencent Cloud will actively cooperate and provide necessary resources and support.
10.2	Information sharing and training	10.2 Cyber risks and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. Insurers should arrange adequate training for all system users on the subject of cybersecurity awareness and	Customers should provide cybersecurity awareness training for all system users and professional skills training for employees responsible for network security and system management. To support customers in meeting regulatory requirements, Tencent has established a Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the latest developments in cybersecurity, taking into account the type and level of cyber risks they may face. Insurers are encouraged to promote the professional competence and capacity of their staff, especially those responsible for cybersecurity and systems.	Technology Committee and specialized security teams across different functions and domains. Internally, Tencent has developed a comprehensive human resources security management standard, including capability and qualification verification before onboarding and role-specific skills training after employment. Tencent Cloud has also implemented a robust information security training mechanism, requiring all formal employees, consultants, interns, and outsourced staff to complete security training courses. These courses include mandatory training for all staff, specialized training for key positions, and elective professional courses. The curriculum covers areas such as basic security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of GL14 Guidelines on Outsourcing



GL14 Guideline on Outsourcing sets out the key considerations that authorized insurers should consider when establishing and overseeing outsourcing arrangements, to safeguard the interests of existing and potential policyholders. The purpose of the guideline is to help authorized insurers identify and mitigate outsourcing risks without compromising operational efficiency. The requirements mainly focus on areas such as service providers, outsourcing agreements, data confidentiality, monitoring and control, contingency planning, and overseas outsourcing arrangements.

In this section, Tencent Cloud summarizes the control requirements in the GL14 Guideline that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists authorized insurers in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
4.2	Legal and Regulatory Obligations	4.2 An authorized insurer must ensure that proper books of account and records are maintained and made available for inspection by the IA in Hong Kong when required, and adequate and up-to-date data can be timely retrieved from the insurer or the service provider. It should not enter into any outsourcing arrangement that would impede the IA's ability to exercise its statutory responsibilities.	Customers must ensure that the Insurance Authority can promptly access or effectively review regulatory records when performing its duties or exercising its powers. Customer data within Tencent Cloud is classified at the highest security level. Customers retain exclusive ownership and control over the content of their data. Tencent Cloud personnel will never proactively access any customer data unless it is necessary for service delivery or troubleshooting, explicit authorization has been granted by the customer, or it is required by national or local government authorities for criminal investigations in accordance with applicable laws and regulations. Tencent Cloud will, based on actual circumstances and the agreements with the customer, cooperate with the customer's third-party security audits and supervision. We will assign dedicated personnel to assist and actively respond to audit activities initiated by the customer. In addition, to support regulatory reviews by financial authorities, Tencent Cloud will respond promptly and provide necessary assistance in accordance with customer requirements.
5.8	Due Diligence	5.8 An authorized insurer should exercise due diligence and care and consider factors such as aggregate exposure to that particular service provider, possible conflict of interest that	Customers should conduct due diligence when selecting a service provider to assess its capabilities and suitability. Tencent Cloud assigns dedicated personnel to respond to customers' due diligence requests

No.	Domain	Summary of Controls	Tencent Cloud's Response
		may arise, and price of the outsourcing vis-à-vis the benefit gained in assessing and selecting a service provider. Besides, when assessing a service provider, it should, among other things, take into account the following factors of the service provider: (a) reputation, experience and quality of service; (b) financial soundness, in particular, the ability to continue to provide the expected level of service; (c) managerial skills, technical and operational expertise and competence, in particular, the ability to deal with disruptions in business continuity; (d) any licence, registration, permission or authorization required by law to perform the outsourced service; (e) extent of reliance on sub-contractors and effectiveness in monitoring the work of sub-contractors; (f) compatibility with the insurer's corporate culture and future development strategies; and (g) familiarity with the insurance industry and capacity to keep pace with innovation in the market.	and, upon request, provides independent third-party audit reports or assurance-based System and Organization Controls (SOC) reports. Below is an overview of Tencent Cloud's capabilities in various aspects of due diligence as a cloud service provider: • **Reputation:** As a cloud computing brand under Tencent, a leading enterprise in China's internet industry, Tencent Cloud has obtained multiple professional certifications from industry organizations, provides comprehensive cloud solutions, and has delivered reliable services to numerous enterprises and government agencies. • **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. • **Management Capability:** Tencent has established a risk governance framework and related procedures, continuously improving risk management measures and internal control systems. Tencent Cloud strengthens its risk culture to enhance internal risk management capabilities and ensure sustainable business development. • **Technical Capability:** Tencent Cloud demonstrates industry-leading technical strength through its robust cloud computing technology, big data processing, AI applications, cybersecurity protection, cloud-native technologies, global data center deployment, and industry-specific solutions. These capabilities ensure service stability and reliability, providing customers with a secure and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			dependable cloud environment. • **Operational Capacity and Scale:** Tencent Cloud's operational capacity and scale are among the leaders in the industry. Its data centers span multiple regions worldwide, including Mainland China, Asia-Pacific, North America, and Europe. Tencent Cloud has partnered with over 11,000 companies and delivered more than 400 industry solutions across 30+ sectors. • **Operational Resilience:** Tencent Cloud is certified under the ISO/IEC 22301 international standard for business continuity management. To ensure service availability, Tencent Cloud has developed detailed disaster recovery plans for its products and services and conducts regular drills to validate timeliness and feasibility. • **Service Qualifications:** Tencent Cloud has provided reliable cloud computing services to numerous international enterprises and government agencies, earning recognition from customers across various industries worldwide. It has obtained more than 400 professional certifications from domestic and international industry organizations, ensuring that its services comply with industry standards and legal and regulatory requirements. • **Subcontractor Management:** If Tencent Cloud engages in subcontracting related business, it will promptly notify the customer and agree on subcontracting terms in the contract based on actual circumstances. Tencent Cloud has established a comprehensive supply chain security management system, which includes strict supplier security assessments and admission processes, regular monitoring and evaluation, and clear outsourcing service agreements, to ensure effective control over suppliers. • **Alignment with Insurers' Corporate**

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Culture and Future Development Strategy: Tencent Cloud has tailored a variety of solutions for numerous institutions in the insurance industry, aiming to flexibly meet the business needs of insurance customers and provide a secure and compliant financial cloud. • **Ability to Keep Pace with Market Innovation:** Tencent Cloud actively tracks market trends and technological developments in the insurance industry, continuously introducing new products and services to maintain its leading position and meet customers' evolving needs. Leveraging advanced technology, user-friendly products, and a strong ecosystem, Tencent Cloud supports industry development on multiple fronts, driving digital-real integration, intelligent upgrades, and innovative convergence.
5.9	Due Diligence	5.9 An authorized insurer should periodically review (at least annually) the ability (including financial strength and technical competence) of the selected service provider to ascertain whether it can continue to provide the expected level of service.	Customers should regularly review the capabilities of their chosen service provider to assess whether its service performance meets the expected standards. Tencent Cloud will cooperate with third-party security audits and supervision based on actual circumstances and contractual agreements, providing dedicated personnel to assist and actively respond to audit activities initiated by customers. Tencent Cloud undergoes regular independent third-party professional audits and provides assurance-based System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulatory authorities, company shareholders, and other relevant stakeholders, disclosing the latest internal control status of Tencent Cloud's service organization. In addition, Tencent Cloud has obtained multiple security and privacy compliance certifications or qualifications, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, CSA STAR, NIST CSF, and SOC,

No.	Domain	Summary of Controls	Tencent Cloud's Response
			demonstrating that Tencent Cloud's security management and personal data protection practices meet relevant certification standards and industry best practices.
5.10	Outsourcing Agreement	5.10 An outsourcing arrangement should be undertaken in the form of a legally binding written agreement.	Customers should enter into an outsourcing agreement with the cloud service provider, clearly specifying the types of outsourced services, service levels, and the responsibilities and obligations of the service provider. The agreement should be subject to regular review. As a cloud service provider, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define matters related to the scope and level of services provided by Tencent Cloud, the protection of user data and intellectual property, the security responsibilities and obligations of both the customer and Tencent Cloud, confidentiality and security requirements, monitoring mechanisms, notifications of incidents and changes, audit and inspection rights, dispute resolution, breach termination and early exit, confidentiality obligations, information disclosure, and applicable laws. Customers may also negotiate including additional requirements in a separate contract.
5.12	Information Confidentiality	5.12 An authorized insurer should ensure that the outsourcing arrangements comply with relevant laws and statutory requirements on customer confidentiality (e.g. the Personal Data (Privacy) Ordinance, Cap. 486 ("PDPO")). The insurer should ensure that it and the service provider have proper safeguards in place to protect the integrity and confidentiality of the insurer's	Customers must comply with the Personal Data (Privacy) Ordinance and relevant guidelines and ensure that both themselves and their service providers have appropriate safeguards in place to maintain the integrity and confidentiality of customer information. 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

No.	Domain	Summary of Controls	Tencent Cloud's Response
		information and customer data.	Security Modules (HSMs) to generate and protect keys and supports key rotation to reduce the risk of compromise or misuse. Invalid, expired, or compromised keys are securely deleted using reliable methods, and once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. Tencent Cloud also employs multi-replica redundant storage and **erasure coding technology** to ensure data integrity and initiate immediate recovery measures upon detecting errors, significantly improving fault tolerance. For **data transmission protection**, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Tencent strictly adheres to laws and regulations related to personal information protection and data security in the jurisdictions where it operates. Tencent has established a user-centric privacy protection framework internally, integrating privacy protection into multiple aspects of corporate culture through comprehensive privacy compliance assessment processes and tools, combining international standards, technological innovation, and employee training, to ensure that customer privacy is protected to the highest degree.
5.13	Data Breach Reporting and Agreement Termination	5.13 An authorized insurer should take into account any legal or contractual obligation to notify customers of the outsourcing arrangement and circumstances under which their data may be disclosed or lost. In the event of the termination of the outsourcing agreement, the insurer should ensure that all customer data	Customers must ensure that, in the event of a customer data breach under an outsourcing arrangement, timely notification is provided to their own customers. In addition, if an outsourcing agreement is terminated, appropriate measures must be taken to retrieve or destroy customer information stored with the service provider. For security incidents that may affect customers, Tencent Cloud will, after internal review and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		are either retrieved from the service provider or destroyed.	based on the scope and severity of the incident, notify customers of the handling and analysis results through appropriate channels and provide technical support to assist customers in taking remedial measures to minimize losses. Tencent Cloud also provides a ticketing service through the Tencent Cloud Console to support customers in reporting faults, incidents, issues, and complaints related to security, availability, and confidentiality. Furthermore, Tencent Cloud offers online customer service and telephone support through the Cloud Console and official website to assist customers with issues encountered while using Tencent Cloud services. If a customer needs to terminate the contract due to business changes or future IT planning, they may choose to back up and migrate cloud data and production environments at any time. According to the service agreement between Tencent Cloud and the customer, if cloud services expire or terminate, the customer must complete data migration before the retention period ends for data stored on Tencent Cloud servers. Tencent Cloud supports customers in backing up and migrating data in standard formats, and customers can use the same transmission methods and protocols as during onboarding, or network services such as **Direct Connect (DC)** and **VPN Connection**, to ensure secure and reliable data migration during offboarding. After service termination, Tencent Cloud will follow strict data erasure procedures to completely delete customer data before reusing previously purchased computing and storage resources.
5.14	Breach of Confidentiality	5.14. An authorized insurer should notify the IA forthwith of any unauthorized access or breach of confidentiality by the service provider or its sub-contractor that affects the insurer or its customers.	Customers must promptly notify the Insurance Authority if a service provider or its subcontractor improperly uses customer information or violates confidentiality requirements. Customer data within Tencent Cloud is classified at the highest security level. Customers retain

No.	Domain	Summary of Controls	Tencent Cloud's Response
			exclusive ownership and control over the content of their data. Tencent Cloud personnel will never proactively access any customer data unless it is necessary for service delivery or troubleshooting, explicit authorization has been granted by the customer, or it is required by national or local government authorities for criminal investigations in accordance with applicable laws and regulations. If an incident involving unauthorized use of customer information or a breach of confidentiality requires reporting to the Insurance Authority, Tencent Cloud will actively cooperate with the customer's needs and provide relevant resource support.
5.15 (c)	Monitoring and Control	5.15 An authorized insurer should ensure that it has sufficient and appropriate resources to monitor and control the outsourcing arrangements at all times: (c) exercise due diligence and care to monitor each outsourcing arrangement to ensure the service is being delivered in the manner 11 expected, and to ensure the provisions included in the outsourcing agreement are properly effected.	To meet customers' outsourcing oversight requirements, Tencent Cloud will cooperate with customers' third-party security audits and supervision based on actual circumstances and the agreements in place, and will assign dedicated personnel to assist, actively responding to and supporting audit activities initiated by the customer. Tencent Cloud also provides online and telephone channels through its official website to support customers in reporting issues encountered while using Tencent Cloud services. Leveraging multi-region backup customer service centers, Tencent Cloud can handle customer inquiries and requests 24/7, delivering high-quality, round-the-clock technical support for cloud products. System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulatory authorities, company shareholders, and other stakeholders, disclosing the latest internal control status of Tencent Cloud's service organization.
5.16	Monitoring and Control	5.16 Once an authorized insurer implements an outsourcing arrangement, it should regularly review the effectiveness and adequacy of its controls in monitoring the performance of the service provider and managing the risks associated with the outsourced service. The insurer should have reporting	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		procedures that can promptly escalate problems relating to the outsourced service to the attention of the management of the insurer and the service provider. It should take appropriate rectification actions forthwith if deficiencies are identified. The insurer is expected to notify the IA forthwith of any significant problem that has the potential to materially affect its financial position, business operation or compliance with legal and regulatory requirements.	
5.17	Contingency Planning	5.17. An authorized insurer outsourcing service to a service provider should put in place a contingency plan to ensure that its business would not be disrupted as a result of undesired contingencies (e.g. systems failure) of the service provider. The following issues should be considered and properly addressed in formulating such contingency plan: (a) back-up facilities or availability of alternative service provider or possibility of bringing the outsourced service back in-house; (b) procedures to be followed and the persons responsible for respective activities if business continuity problem arises; and (c) procedures for regular reviews and testing of the contingency plan.	Customers should maintain and regularly update emergency plans and have a comprehensive understanding of the service provider's business continuity capabilities. Tencent Cloud offers a wide range of products designed with high availability features to help customers achieve system and service resilience. For example: • Cloud Load Balancer (CLB) provides secure and efficient Layer 4 and Layer 7 traffic distribution services, eliminating single points of failure by distributing traffic and expanding application service capacity. CLB uses clustered deployment and promptly removes faulty instances to ensure high availability. • Cloud Virtual Machine (CVM) ensures service availability and data reliability. CVM's cloud disks adopt a three-replica storage strategy, guaranteeing rapid migration and recovery in case of any replica failure. • Cloud Object Storage (COS) provides cross-architecture, multi-device redundant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			storage, enabling disaster recovery and resource isolation for customer data to ensure durability. • **TencentDB for MySQL** supports high reliability and availability with robust automatic backup and lossless recovery mechanisms. • **Tencent Kubernetes Engine (TKE)** uses a distributed architecture to ensure automatic fault recovery and rapid migration. Combined with distributed storage for stateful backend services, it delivers secure and highly available services and data.
5.18	Contingency Planning	5.18 An authorized insurer should also ensure that the service 12 provider has its own contingency plan in respect of daily operational and systems problems. The insurer should have adequate understanding of the service provider's contingency plan and consider the implications for its own contingency planning in the event that the outsourced service is interrupted due to undesired contingencies of the service provider.	To meet regulatory requirements, 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 has obtained ISO/IEC 22301 certification for its Business Continuity Management System. Tencent Cloud conducts business impact analyses for its products and services and develops corresponding strategies and continuity plans to guide resource recovery. To ensure uninterrupted customer operations, Tencent Cloud also formulates detailed disaster recovery plans for its cloud products and conducts regular drills to verify timeliness and feasibility.
5.19	Overseas Outsourcing	5.19 In addition to the essential issues mentioned above, an authorized insurer should pay particular attention to the following issues in relation to overseas outsourcing: (a) Country risk – The country risks associated with overseas outsourcing should be taken into account. Such risks cover	When arranging overseas outsourcing services, customers should consider country-specific risks, the local regulatory authority's rights to access user data, notification obligations, and cooperation with the Insurance Authority's review. Tencent Cloud data centers are distributed across multiple global regions, structured by regions and availability zones, ensuring complete

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the social, economic and political conditions and the legal and regulatory systems of an overseas jurisdiction which may adversely affect the ability of the service provider to carry out the provisions of the outsourcing agreement and the ability of the insurer to effectively monitor the outsourced service and the service provider. (b) Information confidentiality – There may be circumstances under which the insurer's information and customer data are subject to the right of access by an overseas authority (e.g. police and tax authority). The insurer should take into account the extent and possibility of such access right and, as considered appropriate, seek legal advice to clarify the position. In case an overseas authority seeks access to the insurer's customer data, the insurer should forthwith notify the IA. (c) Notification to customers – Having regard to the additional risks posed by overseas outsourcing, the insurer should consider the need to inform their customers of the jurisdiction in which the service is to be performed and any right of access available to overseas authorities. (d) Examination by the IA – The insurer should ensure that, although its service is outsourced to be performed	isolation between regions to maximize stability and fault tolerance. To facilitate local data access and meet compliance requirements regarding data residency, customers can easily specify the desired country or region for data storage through the Tencent Cloud Console when purchasing products. Without customer authorization, Tencent Cloud will never transfer data outside the country or region selected by the customer. Tencent Cloud operates three independent data centers in Hong Kong, each with separate power and network infrastructure, providing a variety of cloud computing services including cloud servers, cloud storage, and cloud databases. These facilities support customers in storing, processing, and backing up data within Hong Kong. Customers may also choose a **Cloud Dedicated Zone (CDZ)**, which can be deployed in a customer-designated facility and offers exclusive resources. Within a CDZ, customers can purchase high-availability resources such as compute, storage, and databases, with an operational experience identical to standard Tencent Cloud availability zones. Tencent Cloud strictly complies with laws and regulations in the jurisdictions where it operates and has established security and compliance programs to ensure information security operations meet legal, regulatory, and industry standards. Before commencing business, Tencent Cloud conducts a comprehensive assessment of the local compliance environment and continuously monitors regulatory developments. Customers retain exclusive ownership and control over their data. Tencent Cloud personnel will never proactively access customer data unless necessary for service delivery or troubleshooting, explicitly authorized by the customer, or required by national or local government authorities for criminal

No.	Domain	Summary of Controls	Tencent Cloud's Response
		outside Hong Kong, such arrangement would not, in any case, impede the ability of the IA to access in Hong Kong the books and records and other information of the insurer as necessary for the IA to carry out its statutory responsibilities. (e) Transfer of personal data – The insurer should pay particular attention to relevant provisions of PDPO if it needs to transfer personal data outside Hong Kong under an overseas outsourcing arrangement.	investigations in accordance with applicable laws and regulations.
5.20	Sub-contracting	5.20 Additional risk will be posed on the risk profile of an authorized insurer if the service provider of the outsourcing arrangement is allowed to further contract the service out to other parties. The insurer should put in place adequate procedures to control and monitor such subcontracting arrangements and ensure that the service provider will take into account the essential issues set out in this Guideline as if it was the insurer concerned when further contracting out the service.	Customers should supervise and manage the subcontracting arrangements of service providers and agree on subcontracting rules and restrictions in the outsourcing agreement. 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 matters related to the scope and level of services provided by Tencent Cloud, the protection of user data and intellectual property, the security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure. If Tencent Cloud engages in subcontracting related business, it will promptly notify the customer and agree on subcontracting terms in the contract based on actual circumstances. Tencent Cloud will actively cooperate with the customer's outsourcing management requirements and respond to audit or assessment activities initiated by the customer. For subcontractor management, Tencent Cloud has established a comprehensive supply chain security management system to ensure effective
5.21	Sub-contracting	5.21 An authorized insurer should incorporate in the outsourcing agreement rules and restrictions on sub-contracting, e.g. requiring insurer's prior consent for sub-contracting and making the service provider liable for the capability of the sub-	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		contractor. The insurer should ensure that its service provider would not engage in sub-contracting arrangement which may impede its ability to carry out the provisions of the outsourcing agreement with the insurer, in particular, the requirements on information confidentiality, contingency planning and information access right by regulator.	control over subcontractors. Tencent Cloud signs formal service agreements with its subcontractors, specifying responsibilities and obligations, including security, privacy, and confidentiality requirements. Through contractual agreements, subcontractors are obligated to comply with these responsibilities. Tencent Cloud also requires subcontractors to submit regular service performance reports and continuously monitors their service levels. Tencent Cloud evaluates subcontractor delivery against agreed security and operational standards and takes appropriate remedial measures for any issues identified to ensure subcontractor performance meets established security and quality requirements.

07 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of GL8 Guideline on the Use of Internet for Insurance Activities

The Hong Kong Insurance Authority (IA) issued the GL8 Guideline on the Use of Internet for Insurance Activities to remind authorized insurers of key considerations when conducting insurance activities online. Section 5.1 of the guideline specifies practical measures that authorized insurers should adopt, focusing on areas such as Internet security policies, information integrity and confidentiality, data backup, and security of electronic payment systems.

In this section, Tencent Cloud summarizes the control requirements in Section 5.1 of the GL8 Guideline that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, assists authorized insurers in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
5.1(a)	Internet Security Policy	(a) a comprehensive set of security policies and measures that keep up with the advancement in internet security technologies shall be in place	Customers should establish comprehensive Internet security policies that are appropriate to the nature of their business. To assist customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy comprising an overarching security strategy, organizational structure, and security management system. This framework effectively supports secure cloud platform operations and risk management, guiding daily work and management processes across departments and employees. Tencent Cloud reviews its information security policy annually to ensure that the objectives, procedures, and controls of its cloud security management system comply with relevant security strategies, standards, procedures, and legal requirements, thereby ensuring adequacy and effectiveness. In addition, Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits and assessments, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, CSA STAR, NIST CSF, and SOC reports. These certifications demonstrate that Tencent Cloud's security management and personal data protection practices meet recognized standards and industry's best practices. Tencent Cloud also undergoes annual audits by professional third-party organizations.

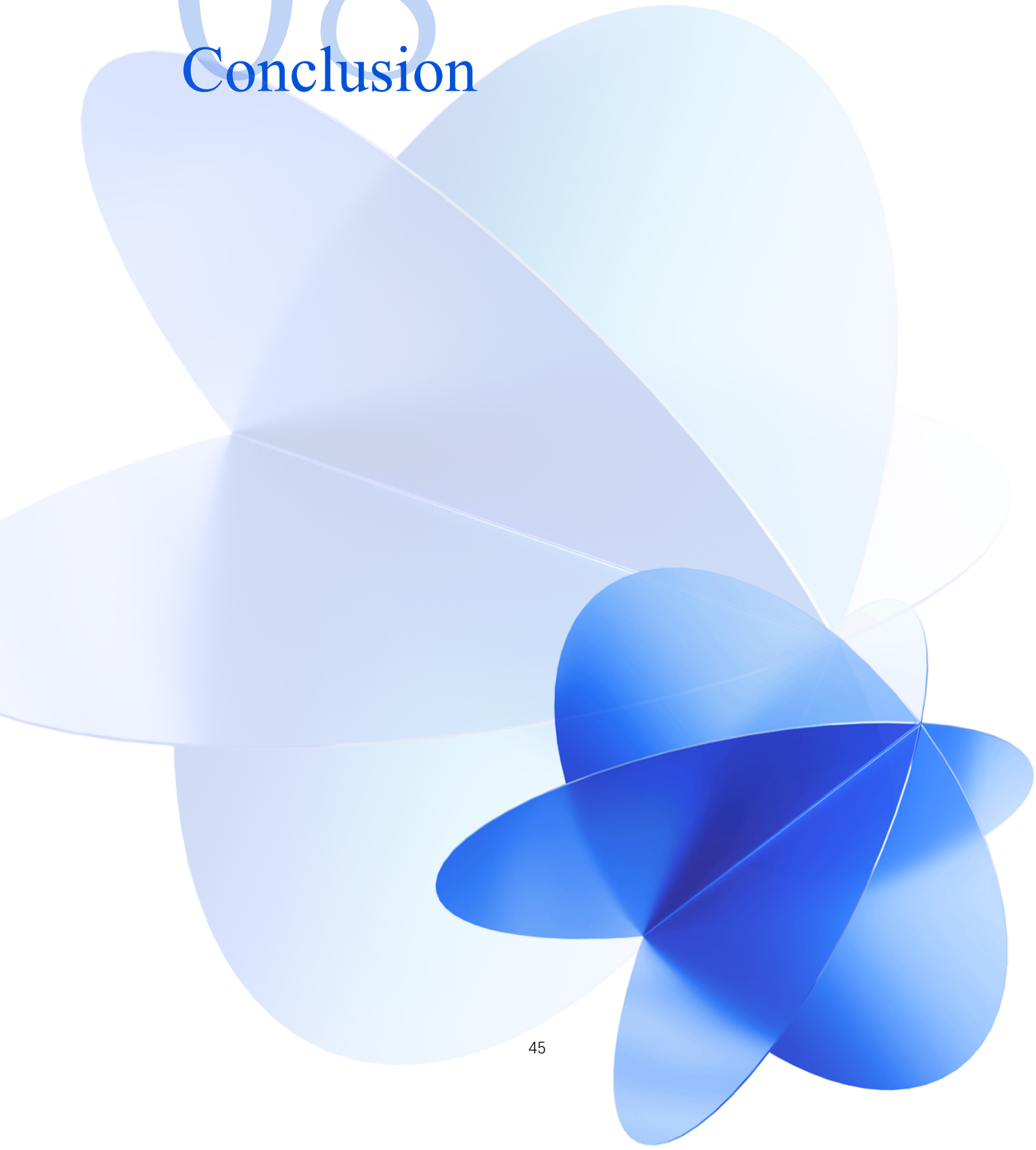
No.	Domain	Summary of Controls	Tencent Cloud's Response
5.1(b)	Information Integrity	(b) mechanisms shall be in place to maintain the integrity of data stored in the system hardware, whilst in transit and as displayed on the website	Customers should implement necessary measures to ensure the integrity of data during storage and transmission. To ensure the confidentiality and integrity of customer data during storage in compliance with regulatory requirements: **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. Invalid, expired, or compromised keys are securely deleted using reliable methods, and once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. Tencent Cloud also employs multi-replica redundant storage and erasure coding technology to ensure data integrity and initiate immediate recovery measures upon detecting errors, significantly improving fault tolerance. **For data transmission protection,** all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • **Direct Connect (DC)**: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • **VPN Connection**: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • Cloud Connect Network (CCN): Enables private network interconnection between cloud VPCs and between VPCs and on-premises data centers (IDCs). CCN supports full-mesh connectivity, dynamic route learning, optimal path selection, and fast convergence in case of link failures. All communication within CCN remains on private networks without traversing the public Internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further guarantees communication quality, making data transmission secure and reliable.
5.1(c)	Backup Management	(c) appropriate backup procedures for the database and application software shall be implemented	Customers should establish a comprehensive backup management mechanism and perform regular backups of databases and application software. Tencent Cloud offers a wide range of storage and database services with built-in backup capabilities to meet diverse customer requirements. Examples include: • Cloud Object Storage (COS): Supports cross-region replication to store data in multiple designated regions, ensuring redundancy and enabling recovery in case of accidental data loss or catastrophic failure in one availability zone. • Cloud Block Storage (CBS): Provides snapshot backup functionality to capture point-in-time snapshots, preventing data loss from tampering or accidental deletion and enabling quick rollback during system failures. • Cloud File Storage (CFS): Offers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			scheduled snapshot capabilities for flexible backup task configuration. • Cloud Native Database TDSQL-C: Supports both logical and snapshot backups, along with binlog backups, allowing restoration of entire clusters or specific tables to any point in time. • TencentDB for MySQL: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability. • TencentDB for MongoDB: Offers automated backup and lossless recovery mechanisms, supporting multi-node backups and retention of multiple days of backup data for disaster recovery scenarios.
5.1(d)	Personal Data Protection	(d) a client's personal information (including password, if any) shall be protected against loss; or unauthorized access, use, modification or disclosure, etc.	Customers should ensure the confidentiality of users' personal data and comply with the requirements of the Personal Data (Privacy) Ordinance. To support customers in meeting regulatory requirements, Tencent strictly adheres to laws and regulations related to personal information protection and data security in the jurisdictions where it operates. Tencent has built a user-centric privacy protection framework, incorporating comprehensive privacy compliance assessment processes and tools, international standards, technological innovation, and employee training. Privacy protection is embedded into multiple aspects of corporate culture to ensure that customer privacy is safeguarded to the highest degree.
5.1(f)	Electronic Payment Systems	(f) the electronic payment system (e.g. credit card payment system) shall be secure	Customers should adopt appropriate protective measures to ensure the security of payment systems. Tencent Cloud has successfully passed PCI DSS certification and obtained Level 1 Service Provider qualification. This demonstrates that Tencent Cloud's infrastructure and physical

No.	Domain	Summary of Controls	Tencent Cloud's Response
			environment meet PCI DSS compliance requirements, enabling Tencent Cloud to provide secure and reliable products and services to support customers' electronic payment systems.

08 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 Insurance Authority (IA) of Hong Kong 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 IA 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.

09 Version History

Date	Version	Detail
April 2026	V1.0	Initial Release