Tencent Cloud

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

April 2026

CONTENTS

CONTENTS

# 01 Overview

The Securities and Futures Commission (SFC), as the regulatory authority for Hong Kong's securities and futures industry, upholds the principles of fairness, transparency, and market stability, and is committed to fulfilling its statutory responsibilities. To guide the healthy development of the market, the SFC has issued a series of regulatory handbooks, guidelines, and circulars with strong advisory value.

With the evolving global market environment and rapid technological advancement, an increasing number of Licensed Corporations[1] engaged in internet-based trading in Hong Kong have begun adopting cloud computing services. This shift presents both significant opportunities and challenges for Hong Kong financial market. In response, the SFC places strong emphasis on enhancing the resilience of the local financial market and strengthening the robustness of market infrastructure. It has issued regulatory requirements for Licensed Corporations in areas such as IT risk management, internet trading security, external electronic data storage, and the use of AI service providers, to ensure compliant operations and effective risk control across the industry.

Tencent Cloud closely monitors regulatory developments and publications from the SFC and is committed to supporting customers in Hong Kong securities and futures industry in meeting these regulatory requirements. This section outlines key SFC guidelines and circulars that Licensed Corporations should pay close attention to, and explains how Tencent Cloud can assist customers in achieving compliance:

- Use of external electronic data storage
- Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading
- Good industry practices for IT risk management and cybersecurity
- Circular to all Licensed Corporations on Internet Trading
- Circular to All Licensed Corporations on Information Technology Management
- Circular to licensed corporations - Use of generative AI language models

[1] A licensed corporation (LC) refers to a corporation that engages in internet-based dealing and is licensed to carry out the following regulated activities: (i) Type 1 regulated activity (dealing in securities); (ii) Type 2 regulated activity (dealing in futures contracts); (iii) Type 3 regulated activity (leveraged foreign exchange trading); and/or (iv) Type 9 regulated activity (asset management), and within that context distributes funds managed by it through its internet trading platform.

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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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).<br>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.<br>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.<br>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.<br><br>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.<br><br>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 Use of External Electronic Data Storage

To provide licensed corporations with greater flexibility in storing regulatory records and to clarify their general responsibilities regarding electronic data, the Securities and Futures Commission (SFC) issued the circular Use of External Electronic Data Storage on 31 October 2019. The circular outlines key requirements for storing regulatory records solely with external electronic data storage providers (EDSPs), as well as the general obligations of licensed corporations when using external data storage or processing services.

In this section, Tencent Cloud summarizes the control requirements relevant to cloud service providers as set out in the circular, and explains how Tencent Cloud, as a cloud service provider, supports licensed corporations in complying with these regulatory expectations.

## 5.1 Requirements for keeping Regulatory Records exclusively with an EDSP

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 7(a)(b) | Selection of Electronic Data Storage Providers | A licensed corporation should ensure compliance with the following requirements if it wishes to keep any Regulatory Records exclusively with an EDSP:<br><br>(a) The EDSP (i) is either a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (Cap 622), in each case staffed by personnel operating in Hong Kong, and (ii) provides data storage to the licensed corporation at a data center located in Hong Kong (Hong Kong EDSP). In addition, the licensed corporation's Regulatory Records which are kept exclusively with the EDSP will be kept at such data center at all times throughout the period in which the Regulatory Records are required to be kept by law or regulation.<br><br>(b) As an alternative, if the EDSP is not a Hong Kong EDSP as defined in paragraph 7(a), the licensed corporation must obtain | If customers intend to store regulatory records with an Electronic Data Storage Provider (EDSP), they must confirm whether the EDSP meets the conditions set out in paragraph 7(a) of the SFC's circular. If the EDSP does not meet these conditions, customers must obtain a written undertaking from the EDSP to provide regulatory records and assistance upon request by the SFC.<br><br>As an EDSP, Tencent Cloud has supported millions of enterprises and individual developers with trusted cloud products and services across various sectors, including gaming, video, mobile, healthcare, public services, finance, and internet-based industries. Tencent Cloud's infrastructure is deployed across multiple global locations, organized into regions and availability zones. Each region is a distinct geographic area, and each availability zone is an isolated failure domain with physical separation. Customers can flexibly deploy their data and systems across different regions or availability zones based on business needs and data security requirements to ensure business continuity and disaster recovery.<br><br>Tencent Cloud operates three data centers within Hong Kong, offering a wide range of cloud computing services such as cloud servers, cloud databases, and CDN. Customers in Hong Kong can choose to store and process their data locally within the region. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | an undertaking by the EDSP, substantially in the form of the template in Appendix 1 (Undertaking) of this circular, to provide Regulatory Records and assistance as may be requested by the SFC. | |
| 7(c) | Selection of Electronic Data Storage Providers | (c) A licensed corporation should only keep Regulatory Records with an EDSP which is suitable and reliable, having regard to the EDSP's operational capabilities, technical expertise and financial soundness. | When selecting an Electronic Data Storage Provider (EDSP), customers should consider the provider's operational capabilities, technical expertise, and financial soundness. Below is an overview of Tencent Cloud's operational capabilities, technical strengths, and financial stability as an EDSP.<br>• **Operational capabilities:**<br>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. Tencent Cloud has established multiple availability zones across various regions, with edge acceleration nodes covering over 70 countries and regions worldwide. This extensive infrastructure ensures high availability, low latency, and robust global service delivery.<br>• **Technical strengths:**<br>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.<br>• **Financial stability:** |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | 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. |
| 7(d) (f) | Access to Regulatory Records | (d) The licensed corporation should ensure that all of its Regulatory Records which are kept exclusively with an EDSP are fully accessible upon demand by the SFC without undue delay, and can be reproduced in a legible form from premises of the licensed corporation in Hong Kong approved for this purpose by the SFC under section 130 of the SFO.<br><br>(f) The licensed corporation should ensure that, irrespective of which EDSP is being used, and of where the EDSP maintains its hardware for the storage of information, Regulatory Records are kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records when it discharges its functions or exercises its powers, taking into account all pertinent political and legal issues in any relevant jurisdiction. | If customers choose to store regulatory records solely with an Electronic Data Storage Provider (EDSP), they must ensure that the SFC can access or retrieve such records promptly and effectively when performing its regulatory functions or exercising its powers.<br><br>As an EDSP, Tencent Cloud offers **Cloud Object Storage (COS)**, which customers can use to store regulatory records in compliance with regulatory requirements. COS is a distributed storage service designed for storing massive volumes of files, allowing users to store and access data over the internet at any time. Customers can manage access permissions for storage buckets and objects. When a request is made for a resource, COS checks the corresponding Access Control List (ACL) to verify whether the requester has the required permissions. By default, resources (buckets and objects) in Tencent Cloud COS are private. Only the primary Tencent Cloud account (resource owner) has access and modification rights. Other users (e.g., sub-accounts or anonymous users) cannot access objects via URL without authorization. Customers can create sub-accounts and assign permissions through access policies, or grant public read access to specific resources (buckets, objects, directories) to allow access by non-Tencent Cloud users. These features enable customers to provide regulatory records to regulators for inspection as required.<br><br>Tencent Cloud is committed to protecting the personal information of customers worldwide and complies with applicable privacy laws in the jurisdictions where it operates. Customer data is |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | classified as the highest level of sensitive data within Tencent Cloud. Customers retain sole ownership and control over their data. Tencent Cloud personnel do not access customer data unless explicitly authorized by the customer for service delivery or troubleshooting purposes, or as required by national or local government authorities in accordance with applicable laws and regulations related to criminal investigations. |
| 7(e) | Recording of Audit Trails | (e) The licensed corporation should ensure that (i) it can provide detailed audit trail information11 in a legible form regarding any access to the Regulatory Records (including read, write and modify) stored by the licensed corporation at the EDSP, and (ii) the audit trail is a complete record of any access by the licensed corporation to Regulatory Records stored by the EDSP. The audit trail information should be kept for the period for which the licensed corporation is required to keep the Regulatory Records. The access of the licensed corporation to the audit trail information should be restricted to read-only. The licensed corporation should ensure that each user who has accessed Regulatory Records can be uniquely identified from the audit trail. | Customers must retain complete and readable records of all access to regulatory records. Additionally, customers must ensure that audit trail data is preserved throughout the required retention period for regulatory records and that such data remains accessible in a readable format.<br><br>Customers may consider using Tencent Cloud's **Cloud Object Storage (COS)** to store their regulatory records. COS provides log management capabilities that record detailed access information for specified source buckets, including user-initiated actions such as uploading, downloading, deleting objects, creating or deleting buckets, and modifying bucket configurations. These logs are stored as files in a designated bucket, enabling better management of storage resources. Logs are generated every five minutes and can be queried and analysed directly using the COS Select feature.<br><br>COS also offers object locking functionality, allowing users to set retention periods during which objects cannot be modified or deleted—meeting strict electronic record retention requirements.<br><br>Additionally, customers can enable real-time logging for buckets using Tencent Cloud's **Cloud Log Service (CLS)**. CLS provides minute-level reporting, real-time search, visualization, and alerting for various object operation logs. Customers can identify authorized account activities on storage buckets using timestamped logs, enabling better access analysis and rapid issue resolution in case of anomalies. Logs collected by CLS can also be delivered to COS for long-term |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | storage, facilitating cost-effective retrieval and analysis. |

## 5.2 General Obligations of Licensed Corporations using External Data Storage or Processing Services

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 12 | Due Diligence | 12. The licensed corporation should conduct proper initial due diligence on the EDSP and its controls relating to its infrastructure, personnel and processes for delivering its data storage services, as well as regular monitoring of the EDSP's service delivery, in each case commensurate with the criticality, materiality, scale and scope of the EDSP's service. Such due diligence should cover:<br><br>(a) the EDSP's internal governance for the safeguard of the licensed corporation's Regulatory Records (where Regulatory Records are kept with the EDSP), and may include assessing the physical security of the storage facilities, the type of hosting (i.e., whether it is dedicated or shared hardware), security over the network infrastructure, IT systems and applications, identity and access management, cyber risk management, information security, data loss and breach notifications, forensics capabilities, disaster recovery and business continuity | Customers should conduct due diligence on Electronic Data Storage Providers (EDSPs) and regularly review their service delivery. The due diligence should cover areas such as physical security, network security, cyber risk management, data security, disaster recovery and business continuity, and subcontractor management.<br><br>Tencent Cloud assigns dedicated personnel to support customers' due diligence requests. Below is an overview of Tencent Cloud's capabilities as an EDSP across key due diligence areas:<br><br>• **Physical Security:**<br>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.<br><br>• **Network Security:**<br>Tencent Cloud designs its network security architecture based on industry best practices, segmenting security zones by business function |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | processes; and<br><br>(b) any subcontracting arrangement by the EDSP for the storage of the licensed corporation's Regulatory Records, especially with regard to cyber risk management and information security. | and risk level, and applying physical or logical isolation. Measures such as access control and perimeter defence ensure the security of office, development, testing, and production networks. Tencent Cloud employs multiple layers of protection including firewalls, IDS/IPS, DDoS mitigation, and web security defences to detect, filter, and block malicious traffic.<br><br>Tencent Cloud also enforces strict access isolation between tenants through virtualization layer controls, private network segmentation, web console access control, session ID and access key validation, ensuring customers can only access their own purchased resources.<br><br>• **IT and Application Security**:<br>Tencent Cloud has established secure development standards for information systems, covering requirement analysis, system design, secure coding, testing, and release. Tencent Cloud integrates ISO/IEC 20000 (IT Service Management), ISO/IEC 27001 (Information Security Management), and ISO/IEC 9001 (Quality Management) standards into the full product development lifecycle, embedding security and privacy protection at every stage—from design to delivery and operations.<br><br>• **Identity and Access Management:**<br>Tencent Cloud has internal access control policies that define account provisioning and deactivation processes, as well as access control requirements for operating systems and applications. Bastion hosts are fully deployed in production environments to centrally manage administrator access to backend systems. Only authorized Tencent Cloud personnel may access these systems, and all access requires multi-factor authentication.<br><br>• **Cyber Risk Management:**<br>Tencent Cloud maintains an internal risk management framework aligned with ISO/IEC 27001:2022 to identify, assess, and manage risks. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | Formal risk assessments are conducted periodically. Risks are evaluated based on likelihood and impact, categorized, and addressed with documented mitigation actions. Residual risks are tracked to ensure proper management by responsible parties.<br><br>• **Information Security:**<br>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.<br><br>• **Data Breach Notification**:<br>Tencent Cloud has established an information security incident management framework, including reporting, response, and handling procedures. For incidents that may impact customers, Tencent Cloud evaluates the scope and severity, notifies affected customers through appropriate channels, and provides technical support to assist with mitigation.<br><br>• **Forensic Support:**<br>Tencent Cloud has defined standards for evidence collection during security incidents. Throughout the incident lifecycle—reporting, investigation, resolution, and follow-up—relevant records are maintained with integrity and confidentiality. Tencent Cloud supports customers with digital forensics and post-incident analysis upon reasonable request. Logs such as access, operation, system, and security event logs are centrally collected, encrypted, and backed up for over one year. These logs are protected from unauthorized modification or deletion and are regularly audited by automated tools and internal audit teams. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | • **Disaster Recovery and Business Continuity:**<br>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 recovery plans are developed. Detailed recovery plans are in place for critical products and processes, with regular drills conducted to ensure timeliness and effectiveness.<br>• **Subcontractor Management:**<br>Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define service scope, data and IP protection, security responsibilities, incident notification, confidentiality, and information disclosure. If subcontracting is involved, Tencent Cloud notifies customers and includes relevant terms in agreements. A robust supply chain security management system ensures effective vendor oversight through strict assessments, onboarding controls, regular evaluations, and formal outsourcing agreements. |
| 14 | Data Protection | 14. The licensed corporation should implement a comprehensive information security policy to prevent any unauthorised disclosure. This policy should include an appropriate data classification framework, descriptions of the various data classification levels, a list of<br>roles and responsibilities for identifying the sensitivity of the data and the corresponding control measures. The licensed corporation should also take appropriate steps to ensure that the EDSP protects Relevant | Customers should establish effective procedures and mechanisms to ensure the confidentiality and security of data stored with Electronic Data Storage Providers (EDSPs). This includes encrypting both data at rest and data in transit, and managing encryption keys throughout their full lifecycle.<br>To ensure the confidentiality and integrity of customer data during storage and to meet 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 |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | Information which is confidential from being intentionally or inadvertently disclosed to, or misused by, unauthorised third parties. To protect its confidential Relevant Information, the licensed corporation should encrypt it while at rest and in transit, or establish effective procedures and mechanisms to safeguard its confidentiality and security. When it is encrypted, the licensed corporation must implement proper key management controls, maintain possession of the encryption and decryption keys and ensure that the keys are accessible to the SFC on demand without undue delay where any electronic record is required to be produced in the exercise of its statutory powers. | 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.<br><br>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:<br>• **Direct Connect (DC)**: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks.<br>• **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.<br>• **Cloud Connect Network (CCN)**: CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal path selection, and fast failover capabilities. All communication within |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | CCN remains off the public internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further enhances communication reliability, making data transmission secure and dependable. |
| 15 | Access Control | 15. The licensed corporation should implement appropriate policies, procedures and controls to manage user access rights to ensure that Relevant Information can only be altered for proper purposes by authorised personnel, and is otherwise free from damage or tampering. The sharing of system authentication codes (such as passwords) among users should generally be prohibited, with a view to ensuring that each user who has accessed Regulatory Records can be uniquely identified. | Customers should establish user access control mechanisms to ensure that only authorized personnel are permitted to access or modify data.<br><br>Tencent Cloud's **Cloud Access Management (CAM)** helps customers securely and precisely manage access to Tencent Cloud products and resources. By default, the primary account has full access to its resources and can create sub-accounts, assign identity credentials, and configure permissions. CAM also supports multiple secondary authentication methods, including MFA devices and SMS verification, to ensure secure identity verification before login or performing sensitive operations.<br><br>Customers can use **CloudAudit** to view and track employee activity logs. CloudAudit supports online access to Tencent Cloud Console and Cloud API operation records for up to 90 days.<br><br>As an Electronic Data Storage Provider, Tencent Cloud does not access or disclose customer content. Customers retain sole ownership and control over their data. To support customers in meeting regulatory requirements, Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator access to backend system components. Access to bastion hosts requires prior authorization and is restricted to designated Tencent Cloud operations personnel. Logging into the bastion host requires appropriate identity verification. All maintenance activities are logged and centrally stored on a secure logging platform, and Tencent Cloud's internal audit team conducts regular |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | reviews of these logs. |
| 16 | Data Monitoring | 16. Where a licensed corporation is keeping only part of its Relevant Information with the EDSP (whether due to data sensitivity concerns or otherwise), it should put in place controls to prevent the migration of Relevant Information to the EDSP without proper authorization. | Customers should establish monitoring measures, including defining data classification requirements and data migration strategies, to prevent the unauthorized transfer of data to an Electronic Data Storage Provider (EDSP) without proper authorization.<br><br>Within Tencent Cloud, customer data is classified as the highest level of sensitive information. Customers retain full control and ownership over their data, and Tencent Cloud does not access or disclose customer content. Adhering to the principle of "data confidentiality," Tencent Cloud employs multi-layered technical isolation mechanisms to ensure that customer data within the same resource pool remains logically segregated. This guarantees that tenants cannot access, retrieve, or tamper with data belonging to other tenants. |
| 17 | Shared Security Responsibility | 17. Public cloud providers and users typically share responsibility for the security and control of the technology, and this may be more complicated than a traditional outsourcing model. Regardless of how the technology is deployed, the licensed corporation should ensure that the allocation of responsibilities, such as the configuration of security settings, workload protection and credential management, | Customers should ensure that security responsibilities are clearly defined and allocated between themselves and the Electronic Data Storage Provider (EDSP).<br><br>To support customers in meeting regulatory requirements, Tencent Cloud adheres to the principles of openness and shared responsibility in cloud computing services. Tencent Cloud continuously enhances the security capabilities of its cloud platform and services, working collaboratively with customers to build a robust and comprehensive security framework for cloud-based operations and data protection.<br><br>As a cloud service provider, Tencent Cloud is |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | between the licensed corporation and the EDSP is well-defined, clearly understood and properly managed by the licensed corporation. Additionally, the licensed corporation may consider using security automation as well as the security services and tools offered by the EDSP to maintain a consistent level of security. | responsible for the security of the underlying data center infrastructure and the cloud platform. Recognizing that control responsibilities vary depending on the type of cloud service selected—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS)—Tencent Cloud has established a Cloud Shared Responsibility Model tailored to different service categories. For more details, please refer to Section 3 "Tencent Cloud's Shared Responsibility Model."<br><br>Based on this model, Tencent Cloud is committed to deepening collaboration with customers to jointly address various security challenges and ensure regulatory compliance. |
| 19 | Business Continuity | 19. A licensed corporation using external data storage or processing services in the conduct of its regulated activities should assess the level of its dependence on the prompt and consistent delivery of services by its service providers as well as the potential operational impact on the licensed corporation and its clients if the services are disrupted. The licensed corporation should establish appropriate contingency plans to ensure its operational resilience, and to require the EDSP to disclose data losses, security breaches, or operational failures which may have a material impact on the licensed corporation's regulated activities. | Customers should assess their level of dependency on the Electronic Data Storage Provider (EDSP) for continuous service delivery, evaluate the potential impact of service disruptions, and establish contingency plans. Customers should also require the EDSP to disclose any security incidents that may have a material impact on their regulated activities.<br><br>As an EDSP, Tencent Cloud is certified under the ISO/IEC 22301 international standard for Business Continuity Management Systems. Tencent Cloud conducts business impact analyses for its cloud products and services and develops corresponding response strategies and business continuity plans to guide the recovery of critical business resources. Detailed disaster recovery plans are in place for cloud products and key processes, and regular drills are conducted to ensure the timeliness and effectiveness of these plans.<br><br>In addition, for security incidents that may impact customers, Tencent Cloud evaluates the scope and severity of the incident and, following internal assessment, communicates the handling and analysis results to affected customers through appropriate channels. Tencent Cloud |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | also provides technical support to assist customers in taking remedial actions to minimize potential losses. |
| 20、21 | Contract Termination | 20. A licensed corporation should have in place an exit strategy to ensure that the external data storage or processing services can be terminated without material disruption to the continuity of any operations critical to the conduct of regulated activities, including in the case of the insolvency of the service provider. If Regulatory Records are stored exclusively with an EDSP, this strategy should clearly outline how a transition to an alternative storage solution (which might include another EDSP) would be executed, and how the SFC's access to Regulatory Records pursuant to the exercise of its regulatory powers will not be impaired during the transition.<br>21. The licensed corporation should have a legally binding service agreement with the EDSP, which should provide for contractual termination. This may include contractual provisions requiring the EDSP to assist in a transition to a new EDSP or allow a migration of data back to storage at the premises of the licensed corporation and, where relevant, clearly delineate the ownership of the data and | Customers should establish an exit strategy to ensure that the termination of external data storage or processing services does not cause significant disruption to business continuity. Contracts with Electronic Data Storage Providers (EDSPs) should include termination clauses, such as transition arrangements and provisions regarding the ownership of data and intellectual property.<br><br>As an EDSP, 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 scope and level of services provided, 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 terms.<br><br>If a customer needs to terminate the service agreement due to business changes or future IT planning, they may back up and migrate their cloud data and production environment at any time. According to the service agreement between Tencent Cloud and the customer, in the event of service expiration or termination, customers are required to complete data migration before the end of the data retention period. Tencent Cloud's cloud supports data backup and migration using standard formats, and 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 migration during offboarding.<br><br>Upon service termination, Tencent Cloud follows strict data erasure procedures to permanently |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | intellectual property following termination of the contract. | delete customer data before reusing any previously allocated computing or storage resources. |

06

# How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

The Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading set out a range of preventive, detective, and other fundamental monitoring requirements to enhance the industry's resilience in cybersecurity. The monitoring measures prescribed in the guidelines are intended to reduce or mitigate hacking risks related to internet trading. The provisions primarily focus on the protection of customers' internet trading accounts, infrastructure security management, and cybersecurity governance and oversight. Licensed or registered persons should implement adequate and effective corresponding measures based on their organizational structure, business operations, and specific needs.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, and explains how Tencent Cloud, as a cloud service provider, supports licensed or registered persons in complying with the relevant requirements.

## 6.1 Protection of Clients' Internet Trading Accounts

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 1.4 | Data Encryption | A licensed or registered person should use a strong encryption algorithm to:<br>(a) encrypt sensitive information such as client login credentials (i.e., user ID and password) and trade data during transmission between internal networks and devices; and<br>(b) protect client login passwords stored in its internet trading system. | Customers should establish effective procedures and mechanisms to ensure the confidentiality and security of data stored with Electronic Data Storage Providers (EDSPs). This includes encrypting both data at rest and data in transit, and managing encryption keys throughout their full lifecycle.<br><br>To ensure the confidentiality and integrity of customer data during storage and to meet 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.<br><br>For **data transmission protection**, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services:<br>• **Direct Connect (DC)**: Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks.<br>• **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.<br>• **Cloud Connect Network (CCN)**: CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal path selection, and fast failover capabilities. All communication within CCN remains off the public internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further enhances communication reliability, making data transmission secure and dependable. |

## 6.2 Infrastructure Security Management

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.1 | Deploy a secure network infrastructure | A licensed or registered person should deploy a secure network infrastructure through proper network segmentation, i.e., a Demilitarized Zone (DMZ) with multi-tiered firewalls, to protect critical | Customers should establish appropriate network isolation measures to configure their network infrastructure, in order to protect critical systems and customer data from cyberattacks.<br>Customers may utilize Tencent Cloud's **Virtual Private Cloud (VPC)** service to build multiple isolated network environments for their |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | systems (e.g., internet trading system and settlement system) and client data against cyber-attacks. | purchased cloud resources. This includes customizable subnet segmentation, IP address allocation, and routing policies. VPC is a dedicated cloud network space built on Tencent Cloud, leveraging tunnelling technology to construct virtual networks over physical infrastructure. Through virtualization, complete internal isolation between different private networks is achieved, providing customers with an independent and secure cloud network environment. Within a private network, customers can configure security groups and network ACL (Access Control List) rules to control inbound and outbound traffic at both the instance and subnet levels, enabling multi-layered network access control.<br><br>Tencent Cloud also offers a suite of security products to help customers establish robust perimeter defences, including:<br><br>• **EdgeOne (EO) platform**: A global edge security and acceleration platform that provides DDoS protection, intelligent web protection, bot/crawler attack mitigation, DNS resolution services, and customizable access control rules based on business needs.<br><br>• **Web Application Firewall (WAF)**: Protects both Tencent Cloud and external users from web-based threats such as attacks, intrusions, vulnerability exploitation, malware injection, tampering, backdoors, and crawlers.<br><br>• **Cloud Firewall (CFW)**: Delivers protection across various network boundaries, addressing unified access control and log auditing requirements in the cloud. It supports proactive ACL management, real-time IPS interception, virtual patching, and malicious code detection. Integrated with Tencent's threat intelligence, it can intercept abnormal |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | outbound connections from hosts in real time. CFW also supports DMZ-like configurations to safeguard core assets and enable fine-grained isolation between VPCs.<br><br>To assist customers in meeting regulatory requirements, Tencent Cloud has deployed a mature network security architecture. This includes firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS mitigation, logical network isolation, and web application security mechanisms to detect, filter, and block malicious traffic in a timely manner, ensuring the security of Tencent Cloud's network.<br><br>At the tenant isolation level, Tencent Cloud enforces strict development and design standards to ensure effective logical separation of customer business data and production environments. This includes virtualization-based isolation, private network access segregation, database instance isolation, and resource-level access control. |
| 2.2 | User access management | A licensed or registered person should have policies and procedures in place to ensure that system access or the use of the systems are granted to users on a need-to-have basis. In addition, a licensed or registered person should review, at least on a yearly basis, the user access list of critical systems (e.g., internet trading systems and settlement systems) and databases (e.g., client data) to ensure that access to or use of the systems remain restricted to persons approved to use them on a need-to-have basis. | Customers should establish user access control mechanisms to ensure that employee access to and usage of systems is properly authorized. In addition, accounts and access rights for critical systems and databases should be reviewed annually.<br><br>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 |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | operation logs to ensure effective traceability of security incidents.<br><br>Tencent Cloud has implemented an access control authorization policy and a permission segregation matrix. Tencent Cloud strictly adheres to the principle of least privilege, with minimum access rights enforced by default. Employees may only obtain specific permissions through a rigorous approval process, and only when necessary for their duties. Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Tencent Cloud maintains records of personnel identity information corresponding to job roles and the permission levels of each business system, and conducts regular internal access reviews to ensure that permissions are not misused or abused. |
| 2.3 | Security controls over remote connection | A licensed or registered person should grant remote access to its internal network on a need-to-have basis and implement security controls over such access. | Customers should grant remote access permissions based on actual business needs and implement appropriate security controls for such access.<br><br>Customers may use Tencent Cloud's **VPN Connection** service to establish secure transmission channels between their on-premises data centers and Tencent Cloud resources. The VPN tunnel uses IKE (Internet Key Exchange) and IPsec protocols to encrypt data in transit, creating a secure and trusted data tunnel over the Internet to ensure data security during transmission. The VPN gateway is highly reliable, built on an active-standby architecture to ensure uninterrupted communication sessions and seamless application experience.<br><br>To facilitate secure and fast access to cloud-based business systems from any location, at any time, and using any mainstream device, Tencent Cloud supports SSL VPN remote access technology. SSL VPN encrypts data transmitted over the Internet and supports access control mechanisms |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | to reduce unauthorized access.<br><br>Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect via encrypted communication channels to access Tencent Cloud's corporate network and daily operational systems. Tencent Cloud maintains remote access logs to record user activities.<br><br>Furthermore, Tencent Cloud's internal corporate 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 multi-factor authentication (MFA). During permission assignment, Tencent Cloud enforces fine-grained access control, ensuring that employees are granted only the minimum permissions necessary to perform their duties. Any request for additional permissions must undergo multi-level review and approval. All backend operational activities are logged and centrally stored on a logging platform, which is regularly audited by Tencent Cloud's internal audit team. |
| 2.4 | Patch management | A licensed or registered person should monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing. | Customers should continuously monitor and assess the release of software patches from vendors, evaluate their potential impact, conduct testing, and install patches promptly upon completion of testing.<br><br>**To assist customers with vulnerability remediation and asset risk management**, Tencent Cloud provides the **Cloud Security Center (CSC)**. CSC enables unified security management of cloud assets, including automated asset inventory, detection and identification of various security risks, and automated response to asset-related threats. Leveraging Tencent's threat intelligence |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | capabilities, CSC delivers timely notifications of newly discovered vulnerabilities along with detailed reports outlining the scope of impact and recommended remediation actions, helping customers quickly detect and address high-risk vulnerabilities.<br><br>CSC also supports automated response orchestration, allowing customers to preconfigure workflows that enhance threat response efficiency.<br><br>**For container vulnerability management**, Tencent Cloud Container Security Service (TCSS) regularly scans local and repository images for vulnerabilities, retrieves real-time vulnerability data from official sources, and maintains an up-to-date vulnerability database.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established both internal and external vulnerability identification mechanisms. For external vulnerabilities, Tencent Cloud operates a coordinated vulnerability reward program centered around the Tencent Security Response Center (TSRC). This program leverages crowdsourced testing by white-hat researchers, AI-driven threat intelligence analysis, and multi-dimensional validation processes to systematically identify vulnerabilities across cloud products and core business systems.<br><br>For internal environments, Tencent Cloud uses vulnerability scanning systems to regularly scan cloud assets. Identified vulnerabilities are communicated via security tickets to relevant departments for evaluation and remediation. All vulnerabilities must be resolved and verified within the designated timeframe. |
| 2.5、2.6 | End-point protection | 2.5 A licensed or registered person should implement and update anti-virus and anti-malware solutions (including the corresponding definition | Customers should establish procedures and implement controls to detect and prevent computer viruses or other malicious software attacks targeting software and information |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | and signature files) on a timely basis to detect malicious applications and malware on critical system servers and workstations.<br>2.6 A licensed or registered person should implement security controls to prevent unauthorised installation of hardware and software. | processing facilities.<br><br>Customers can use **Cloud Workload Protection Platform (CWPP)** to secure cloud servers. CWPP leverages Tencent's extensive threat intelligence and machine learning to provide intrusion detection, vulnerability risk alerts, and other security services, including password cracking prevention, abnormal login alerts, Trojan file detection, and high-risk vulnerability detection, addressing major cybersecurity risks faced by servers.<br><br>**To help customers meet regulatory requirements for server virus protection**, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage all server endpoints. The EDR solution supports antivirus and intrusion detection, security baseline and vulnerability scanning, as well as compliance auditing of command operations and login activities. It triggers alerts upon detecting malicious programs or abnormal behaviors.<br><br>**For personal computer usage management**, Tencent Cloud has established software security standards that define restrictions on software usage on personal computers (including laptops and workstations). Application whitelisting technology is used to allow only known and trusted programs to run, reducing the risk of malware intrusion. Tencent Cloud also uses a Zero Trust Security Management System to manage personal computer endpoints, providing capabilities such as virus removal, vulnerability remediation, and proactive defense to deliver comprehensive protection against ransomware, phishing attacks, and lateral movement threats. |
| 2.7 | Physical security | A licensed or registered person should establish physical security policies and procedures to protect critical system components (e.g., | Customers should establish physical security management policies and procedures to prevent unauthorized personnel from accessing critical system infrastructure.<br><br>To support customers in meeting regulatory |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | system servers and network devices) in a secure environment and to prevent unauthorised physical access to the facilities hosting the internet trading system as well as the critical system components. | requirements, Tencent Cloud has implemented strict physical access control policies across its data centers, tailored to the security requirements of different zones. All visitors and personnel entering data centers must undergo identity verification, inspection of personal belongings, and registration of carried items. Based on personnel categories and access permissions, Tencent Cloud maintains a comprehensive access control matrix within its data center authorization system to effectively manage access and operational activities.<br><br>In Tencent Cloud's financial zones, physical server rooms are equipped with dedicated cages to isolate customer equipment, and biometric access control systems are deployed to prevent unauthorized access to customer assets.<br><br>**Regarding data center security and monitoring**, Tencent Cloud's security personnel conduct inspections of server rooms and equipment in accordance with predefined checklists and schedules. Each inspection point requires signature and timestamp logging. In the event of infrastructure failure or a security incident, Tencent Cloud immediately activates its data center emergency response procedures. All data centers are equipped with 24/7 video surveillance systems with full coverage and alert capabilities, monitored by security staff. Surveillance footage is securely stored and retained for an appropriate duration. |
| 2.8 | System and data backup | A licensed or registered person should back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis.<br>A licensed or registered person should also adopt an appropriate recovery method | Customers should also regularly back up business records, customer or transaction data, and documents, and implement a backup and recovery solution.<br><br>Tencent Cloud currently operates three independent data centers in Hong Kong, each with separate power and network infrastructure, enabling customers to store, process, and back up data locally within Hong Kong. Tencent Cloud offers multiple storage and database services |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | to enable successful roll-back of major system changes. | with built-in backup capabilities to meet diverse customer needs, such as:<br>• 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.<br>• 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.<br>• Cloud File Storage (CFS): Offers scheduled snapshot capabilities for flexible backup task configuration.<br>• 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.<br>• TencentDB for MySQL: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability.<br>• 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.<br>To ensure the continuous availability of customer business operations, Tencent Cloud has developed detailed disaster recovery plans for its cloud products and critical processes. These plans are regularly tested in accordance with defined requirements to ensure their timeliness and effectiveness. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.9 | Contingency planning for cybersecurity scenarios | In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, a licensed or registered person should make all reasonable efforts to cover possible cyber-attack scenarios such as distributed denial-of-service (DDoS) attacks2 and total loss of business records and client data resulting from cyber-attacks (e.g., ransomware) in the contingency plan and crisis management procedures. | Customers should establish a security incident response management procedure to ensure timely and effective response in the event of a cyberattack.<br>To support customers in meeting regulatory requirements, Tencent Cloud has developed a Cybersecurity Incident Response Plan covering a wide range of scenarios including cyberattacks, malware, data security incidents, equipment failures, and disaster events. The plan is built on a comprehensive emergency response framework, supported by dedicated response teams, and emphasizes standardized incident handling procedures. This enhances Tencent Cloud's capabilities in monitoring, alerting, and coordinated response to minimize the impact of cybersecurity incidents.<br>Relevant internal departments at Tencent Cloud regularly conduct training and simulation exercises based on the emergency response plan. In addition, Tencent Cloud provides ongoing technical training to its security teams in line with evolving security technologies and threat landscapes. This ensures that personnel are familiar with and adhere to the latest security policies and operational procedures, are equipped with up-to-date information security standards and best practices and can respond swiftly and effectively when incidents occur. |

## 6.3 Cybersecurity Management and Supervision

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 3.2 | Cybersecurity incident reporting | A licensed or registered person should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (e.g., to the responsible officer(s) or | Customers should establish a mechanism for reporting security incidents, clearly defining the reporting procedures and designated recipients for cybersecurity incidents.<br>To support customers in meeting regulatory requirements, Tencent Cloud has developed an Information Security Incident Management Policy, which includes procedures for incident response, escalation, and notification. These |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | executive officer(s) in charge of internet trading) and externally (e.g., to clients, the SFC and other enforcement bodies, where appropriate). | procedures ensure timely alerts or notifications to internal personnel, customers, and other relevant stakeholders who may be affected by the incident, enabling orderly, timely, and efficient communication and coordination.<br><br>For security incidents that may impact customers, Tencent Cloud will assess the scope and severity of the incident and, following internal review, notify customers of the incident handling and analysis results through appropriate channels. Tencent Cloud will also provide technical support to assist customers in implementing remedial measures to minimize potential losses.<br><br>In the event that a customer experiences a cybersecurity incident that requires reporting to the Securities and Futures Commission (SFC), Tencent Cloud will actively cooperate with the customer's needs and provide the necessary resources and support. |
| 3.3 | Cybersecurity awareness training for internal system users. | A licensed or registered person should provide adequate cybersecurity awareness training to all internal system users at least on a yearly basis. When designing the content of the training programme, the licensed or registered person should take into account the type and level of cybersecurity risks it faces. | Customers should establish a cybersecurity awareness training mechanism and conduct regular training sessions for internal staff.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Program. This program mandates participation from full-time employees, consultants, interns, and outsourced personnel. The training includes mandatory courses for all staff, specialized training for key roles, and elective professional courses. Topics covered include basic security awareness, office security, vulnerability identification and mitigation, privacy protection, incident response, secure development practices, and data security requirements. |

07

# How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Good Industry Practices for IT Risk Management and Cybersecurity

The Good Industry Practices for IT Risk Management and Cybersecurity provide licensed corporations engaged in internet trading with a reference checklist of industry best practices. Licensed corporations are encouraged to incorporate these practices into their cybersecurity and IT risk management frameworks. The provisions primarily cover areas such as overall cybersecurity governance, system and network infrastructure security, security monitoring and capacity management, system development and change management, cybersecurity risk assessment, data backup and contingency planning, and vendor management.

In this section, Tencent Cloud summarizes and extracts the control requirements relevant to cloud service providers as outlined in the Good Industry Practices for IT Risk Management and Cybersecurity, and explains how Tencent Cloud, as a cloud service provider, supports licensed corporations in complying with the relevant requirements.

## 7.1 General Cybersecurity Governance

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| A3 | Threat Intelligence | Subscribe to cyber intelligence sources for pre-emptive monitoring of emerging cyber threats. | Customers should subscribe to threat intelligence from multiple sources to conduct proactive assessments of emerging cybersecurity threats.<br><br>To support customers in threat detection and analysis, Tencent Cloud provides the **Threat Intelligence Center (TIX)** — a one-stop intelligence service platform offering foundational intelligence, attack surface intelligence, and business intelligence capabilities. TIX supports intelligence queries, IOC (Indicators of Compromise) analysis, and attack surface management, helping customers efficiently analyze security incidents and comprehensively assess the exposure risks of enterprise assets, thereby enabling the construction of a robust and multi-layered security defense system.<br><br>The Threat Intelligence Center aggregates intelligence from a wide range of sources, including vulnerability communities, security organizations, security tool vendors, social media, and security blogs. It leverages cloud-based algorithms to eliminate false positives, ensuring the accuracy of the intelligence provided.<br><br>TIX is built around a SaaS-based delivery model and supports multiple integration methods including Web APIs, SDKs, TIPs (Threat Intelligence Platforms), and mini-programs to |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | meet diverse customer needs. It can also be integrated with customers' existing security products to enhance overall security operations and threat response efficiency.<br><br>Empowered by the Threat Intelligence Center, Tencent Cloud is committed to building a proactive defense capability framework encompassing intelligence, offense-defense, management, and planning. By integrating threat intelligence, artificial intelligence, and big data technologies, Tencent Cloud enhances its ability to respond to security incidents. A 24/7 Security Operations Center (SOC) has been established to focus on threat detection, investigation, and response, enabling visibility, awareness, and control over the security landscape.<br><br>Customers should also establish a cybersecurity awareness training mechanism and conduct regular training sessions for internal staff.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Program. This program requires participation from full-time employees, consultants, interns, and outsourced personnel. Training offerings include mandatory courses for all staff, specialized training for key roles, and elective professional modules. Topics covered include basic security awareness, office security, vulnerability identification and mitigation, privacy protection, incident response, secure development practices, and data security requirements. Some training sessions include security assessments, and employees must pass these assessments to be considered as having completed the course, ensuring familiarity with Tencent Cloud's internal cybersecurity policies and requirements. |
| A5 | Cybersecurity Training | Equip staff with the right skills, the right knowledge and the right behavior and ensure key | Customers should establish a cybersecurity awareness training mechanism and conduct regular training sessions for internal staff. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | staff, especially those responsible for IT Security Operations and Delivery, IT Risk Management and Control and IT Audit, have relevant professional qualifications, training and experience. | To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Program. This program mandates participation from full-time employees, consultants, interns, and outsourced personnel. The training includes mandatory courses for all staff, specialized training for key roles, and elective professional courses. Topics covered include basic security awareness, office security, vulnerability identification and mitigation, privacy protection, incident response, secure development practices, and data security requirements. |

## 7.2 Secure System and Network Infrastructure

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| B1 | Network Segmentation | Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. In particular, control and protect sensitive data traffic between different network segments. | Customers should segment their networks and implement access control measures for connections between different zones, based on the sensitivity of data and systems.<br><br>Customers can use Tencent Cloud's **Virtual Private Cloud (VPC)** service to create multiple isolated network spaces for purchased cloud resources, with customizable IP ranges and routing policies. VPC uses tunneling technology to build virtual networks on physical infrastructure, achieving complete logical isolation between private networks. Within a VPC, customers can configure security groups and network ACL rules to control inbound and outbound traffic at both instance and subnet levels, enabling multi-layered network access control.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established strict internal network isolation policies. These policies enforce access control and perimeter protection across various internal environments—including corporate, development, testing, and production networks— |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | through both physical and logical isolation mechanisms. |
| B2 | Network Infrastructure Security | Set up the Demilitarized Zone (DMZ) with robust security controls by:<br>- Deploying multi-tiered firewalls of different brands and types to control and filter network traffic between the DMZ and the trusted internal networks;<br>- Implementing Intrusion Prevention System, Web Application Firewall, anti-APT (Advanced Persistent Threat) solutions to protect the internet-facing servers in the DMZ;<br>- Deploying Intrusion Detection System (IDS) and System Information & Event Management (SIEM) solutions to detect and monitor unauthorised access and data transfer;<br>- Not storing or catching sensitive data such as customer login credentials within the DMZ; and<br>- Protecting sensitive data through strong encryption during transmission within the DMZ. | Customers should establish demilitarized zones (DMZs) within their network architecture and deploy network security monitoring solutions such as firewalls, intrusion prevention systems (IPS), and web application firewalls (WAF) to monitor and filter communications between network segments.<br>Tencent Cloud also offers a suite of security products to help customers establish robust perimeter defences, including:<br>• **EdgeOne (EO) platform**: A global edge security and acceleration platform that provides DDoS protection, intelligent web protection, bot/crawler attack mitigation, DNS resolution services, and customizable access control rules based on business needs.<br>• **Web Application Firewall (WAF)**: Protects both Tencent Cloud and external users from web-based threats such as attacks, intrusions, vulnerability exploitation, malware injection, tampering, backdoors, and crawlers.<br>• **Cloud Firewall (CFW)**: Delivers protection across various network boundaries, addressing unified access control and log auditing requirements in the cloud. It supports proactive ACL management, real-time IPS interception, virtual patching, and malicious code detection. Integrated with Tencent's threat intelligence, it can intercept abnormal outbound connections from hosts in real time. CFW also supports DMZ-like configurations to safeguard core assets and enable fine-grained isolation between VPCs.<br>• **VPN Connection**: enables customers to |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | establish secure transmission channels between their on-premises data centers and Tencent Cloud resources. The VPN tunnel uses IKE (Internet Key Exchange) and IPsec protocols to encrypt data in transit, creating a secure and trusted data tunnel over the Internet to ensure data security during transmission.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has designed its network security architecture based on industry best practices. Security domains are segmented according to business functions and risk levels, with physical and logical isolation applied to ensure the security of corporate, development, testing, and production networks. Tencent Cloud employs multiple layers of protection—including firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS mitigation, and web security defenses—to detect, filter, and block malicious network traffic in a timely manner, safeguarding the integrity of Tencent Cloud's network. |
| B3、B4 | Secure Configuration | B3 Implement secure configuration of key IT systems, i.e. system hardening. Disable or remove any unused programs, ports, computer processes and privileged accounts.<br>B4 Implement application whitelisting solutions to prevent installation of unauthorized applications on users' computers or servers. | Customers should implement secure configurations for key IT systems and deploy application whitelisting solutions to prevent unauthorized applications from being installed on user devices or servers.<br><br>Customers may adopt **Cloud Workload Protection Platform (CWPP)**, a service powered by Tencent's extensive threat intelligence, to manage baseline security. CWPP supports baseline detection through one-click and scheduled scanning modes, provides visibility into baseline compliance rates, and offers remediation recommendations. Tencent Cloud also provides default baseline policies to help customers manage server security more effectively.<br><br>The **Cloud Security Center (CSC)** offers automated configuration risk assessment across various cloud products—including cloud servers, |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | object storage, cloud databases, and load balancers—helping customers reduce security risks caused by misconfigurations and improve overall cloud security posture. Additionally, customers can use **Configuration Audit (Config)** for centralized auditing and governance of cloud resources, continuously recording configuration data and changes across regions under their account. Based on Tencent Cloud's best practices and compliance templates, Config performs ongoing compliance assessments to identify non-compliant configurations and enable automated monitoring and management.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established standardized **network security configuration and baseline standards** for network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud uses scanning tools to continuously detect deviations between actual configurations and defined standards across operating systems, database management systems, network devices, and virtual images. Identified deviations trigger automated security tickets sent to responsible teams for timely remediation. Tencent Cloud also regularly reviews the security policies and parameter settings of routers, firewalls, and network servers to ensure their effectiveness.<br><br>For **endpoint protection**, Tencent Cloud has defined software security policies that restrict software usage on personal computers (including laptops and workstations). Application whitelisting technology is used to allow only known and trusted programs to run, reducing the risk of malware intrusion.<br><br>At the **host security** level, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to monitor and manage server assets across the network. The EDR solution supports antivirus and intrusion detection, baseline and vulnerability scanning, and compliance auditing |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | of command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviour, and incidents are tracked and handled via Tencent Cloud's ticketing system. Tencent Cloud also regularly reviews and updates EDR security policies, including user access and system access controls. |
| B5、B6 | Anti-DDoS attack | B5 Assess the risk of Distributed Denial of Service (DDoS) attacks and implement anti-DDoS mechanisms and solutions by filtering high volume and suspicious incoming traffic/cyber-attacks as appropriate.<br>B6 Review the network architecture and properly configure the Domain Name System (DNS) and/or Network Time Protocol (NTP) servers in order to prevent criminals from launching reflective amplification DDoS attacks. | Customers should assess the risk of Distributed Denial-of-Service (DDoS) attacks and implement effective DDoS mitigation mechanisms and solutions. In addition, customers should strengthen the security of internal Domain Name System (DNS) and Network Time Protocol (NTP) servers through technical and administrative controls.<br>Customers may use Tencent Cloud's **Anti-DDoS** service to mitigate DDoS risks. This service combines robust and high-quality DDoS protection resources with continuously evolving proprietary and AI-driven traffic scrubbing algorithms to ensure the stable and secure operation of customer services. Anti-DDoS offers multiple protection solutions, including basic DDoS protection for cloud servers and load balancers, which supports real-time traffic monitoring and attack mitigation for daily security operations. For industries requiring high availability and reliability, Tencent Cloud provides enhanced protection services such as Anti-DDoS Advanced IP, which helps prevent service disruptions and financial losses caused by large-scale DDoS attacks.<br>Customers may also opt for **EdgeOne DDoS Protection**, delivered via Tencent Cloud's Edge Security Acceleration Platform. EdgeOne uses Anycast routing technology to provide edge-level security and supports L3/L4 volumetric DDoS protection. It monitors traffic in real time and initiates scrubbing upon detection of an attack. EdgeOne's DDoS protection features include predefined defence policies based on attack profiling, behavioural analysis, and AI-powered |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | detection algorithms. For businesses with high DDoS risk exposure, long-lived connections, or custom traffic control needs, EdgeOne offers dedicated DDoS protection through exclusive scrubbing centers to meet advanced filtering requirements.<br><br>**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 mitigation tools, and conducts regular DDoS protection drills.<br><br>Tencent Cloud also monitors abnormal DNS queries in real time (e.g., high-frequency requests or irregular domain patterns). All services must use Tencent Cloud's designated internal DNS service, and unauthorized public DNS usage is prohibited. Tencent Cloud ensures that all relevant infrastructure is synchronized with accurate time sources, and its data centers regularly verify the synchronization status of their NTP servers. |
| B7 | System Resilience | Design the internet trading system and underlying technology architecture with sufficient system resilience considerations, e.g. high availability server clusters, multiple network connections (preferably from different carriers), redundancy of critical hardware or equipment. | Customers should fully consider system resilience when designing internet trading systems and related technical architectures.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud operates data centers across multiple global regions. Each availability zone connects to multiple network carriers, enabling cross-regional disaster recovery capabilities and effectively reducing the impact of public network failures. Tencent Cloud's core network infrastructure is built using a redundancy model, combined with routing-level traffic engineering, path prioritization, and route reachability mechanisms to ensure uninterrupted network services in the event of single-point device failures.<br><br>Tencent Cloud's compute nodes also follow a redundancy design. If a single compute node fails, the scheduler automatically removes it in |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | real time, ensuring the availability of customer services. |

## 7.3 System Access Control and Data Protection

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| C1、C2、C3 | Access Management and Privileged Account Management | C1 Establish formal access management and privileged account management procedures with adequate checks and balances. Control, record and monitor all access to end point devices, servers and network equipment using privileged or emergency accounts. Implement Identity Access Management (IAM) and Privileged Access Management (PAM) tools to help ensure the consistent implementation of access management practices.<br>C2 Limit privileged user access to operating systems to prevent installation of malicious applications, unauthorized manipulation of system configurations or removal of security tools on users' computers or servers.<br>C3 Do not allow system development personnel (including vendors) to have access to the production environment without prior written senior management's approval, supported by explanation. Where access to the production environment is | Customers should establish access control and privileged account management procedures to record and monitor access to endpoints, servers, and network devices. The use of privileged accounts should be restricted to prevent unauthorized installation or modification activities.<br>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.<br>Customer data is classified as the highest security level 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 implemented comprehensive operational security mechanisms to ensure that its service teams cannot directly access customer information assets without the customer's explicit consent and authorization.<br>To support customers in meeting regulatory |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | allowed, put in place a mechanism to record and monitor such activities. | requirements, Tencent Cloud's internal corporate network is completely isolated from the production environment where customer data resides. Operations personnel must access the production environment via bastion hosts, and all operational accounts are equipped with multi-factor authentication (MFA). During permission assignment, Tencent Cloud enforces fine-grained access control, ensuring that employees are granted only the minimum permissions necessary to perform their duties. Any request for additional permissions must undergo multi-level review and approval. All backend operational activities are logged and centrally stored on a logging platform, which is regularly audited by Tencent Cloud's internal audit team. |
| C3、C4 | Key Management | C3 Establish formal cryptographic key management policy and procedures to govern the life cycle of cryptographic keys for the encryption of confidential and sensitive data.<br>C4 Implement data protection controls by adopting system login passwords that are salted and one-way hashed, preferably with a slow hash function. | Customers should establish password management policies and procedures and implement full lifecycle management for cryptographic keys.<br><br>To protect login credentials, customers may use **Cloud Access Management (CAM)** to configure password policies for sub-users via the CAM console, including settings for password complexity, length, and expiration. To prevent password leakage, Tencent Cloud applies SHA-256 hashing and salting techniques to encrypt passwords, avoiding plaintext storage.<br><br>The **Key Management Service (KMS)** provides full lifecycle management of cryptographic keys, utilizing FIPS 140-2 certified Hardware Security Modules (HSMs) for key generation and protection. KMS supports diverse key management needs across multiple applications and business scenarios. For financial institutions, where communication and stored data are highly sensitive and valuable, KMS offers envelope encryption to secure protocol communications, critical documents, and data, while also managing key permissions to meet security and compliance requirements. To reduce the risk of key compromise or misuse, KMS supports key |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | rotation and provides secure methods for deleting expired, revoked, or compromised keys. Deleted keys are unrecoverable, and any data encrypted under those keys becomes permanently inaccessible.<br><br>Tencent Cloud has established security management standards for encryption algorithm usage and key lifecycle management. These standards define secure procedures for key application, generation, storage, usage, transmission, rotation, and destruction. All key-related operations follow strict requirements for dual control, secure handover, proper storage, and timely updates. During key usage, Tencent Cloud enforces segregation of duties, strict approval processes, and authenticated operations, with all key activities logged and subject to regular audits.<br><br>During data transmission and storage, Tencent Cloud requires internal teams to comply with international cryptographic standards and regulations, using high-security algorithms such as AES-256, and ensuring key lengths meet required specifications. |
| C6、C7 | Information Protection | C6 Define, identify, document and protect data flow of sensitive information and deploy data protection processes and technologies (e.g. Data Loss Prevention solutions) to provide adequate coverage and trigger appropriate responses<br>C7 Establish policies and procedures for information security, apply data protection and baseline security controls to different data classifications, based on level of sensitivity and criticality; and procedures for disposal of confidential documents and destruction of | Customers should establish mechanisms for information security protection, classify data based on its sensitivity and importance, and implement appropriate data protection measures according to its classification level. In addition, customers should define procedures for securely erasing confidential files and physical devices.<br><br>The **Data Security Governance Center (DSGC)** 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 |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | physical devices to prevent data leakage. | 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.<br><br>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 at the highest security level within Tencent Cloud. Customers retain sole ownership and control over their data. Tencent Cloud employees do not access customer data unless required by the services selected by the customer.<br><br>Upon termination of cloud services, Tencent Cloud follows strict data erasure procedures. After the retention period expires, all customer data—including backups and replicas—is permanently deleted and cannot be recovered. If the physical media used to deliver Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud performs secure physical destruction in accordance with rigorous protocols. |

## 7.4 Security Monitoring and Capacity Management

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| D1、D2、D5 | Logging and Security Monitoring | D1 Establish a Security Operations Center (SOC) or equivalent function with sufficient resources to take charge of all security monitoring processes and | Customers should establish a Security Operations Center (SOC) to detect malicious activities and ensure that operational records of computer and network systems are retained and audited.<br><br>Customers may use Cloud Log Service (CLS), a one-stop logging platform that supports log |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | technologies and act as a coordinator for efficient incident detection and handling.<br>D2 Tailor behavioural monitoring solutions and their underlying parameters to enable detection of malicious activities.<br>D5 Maintain and review audit trail records / access logs for computers or network systems to identify any unauthorised access attempts or system security attacks. | 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.<br><br>Customers can also use **CloudAudit** to record logs and continuously monitor account activity across Tencent Cloud infrastructure. **Elasticsearch Service (ES)** enables customers to stream real-time logs from cloud servers, containers, and other cloud products, as well as ingest historical and incremental business data into Tencent Cloud ES clusters for distributed storage and analytical queries.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established a Security Operations Center based on cloud-native technologies, focusing on threat detection, investigation, and response. The SOC operates 24/7 and is staffed by professional teams capable of promptly handling security alerts, conducting preliminary analysis, and formulating containment strategies to prevent attacks or incidents.<br><br>Leveraging years of experience in anomaly detection, Tencent Cloud has built a comprehensive rule base that triggers real-time alerts for suspicious activities. Tencent Cloud also enforces strict operational security policies and conducts regular internal reviews. All backend operational activities in the production environment are thoroughly logged and centrally stored on a logging platform, with periodic audits conducted by Tencent Cloud's internal audit team.<br><br>Tencent Cloud has also deployed internal network |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | monitoring systems to oversee routers, firewalls, and network servers, generating alerts for anomalies and tracking resolution through its ticketing system. |
| D7、D8 | Capacity Management | D7 Establish performance alert thresholds, for example, CPU usage, memory usage, disk I/O and free space, bandwidth to facilitate monitoring of system and network activities.<br>D8 Implement alert mechanism to timely notify the relevant parties for corrective actions when approaching performance alert thresholds. | Customers should establish a system performance management mechanism, including setting performance alert thresholds. When system performance exceeds the defined thresholds, alerts should be triggered.<br><br>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.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud conducts capacity forecasting based on business operational needs and formulates an annual capacity management plan. While ensuring business continuity of information systems, business units reference historical monitoring data to identify usage trends and incorporate anticipated demands from new services and systems into capacity planning.<br><br>During daily operations, Tencent Cloud's internal teams use a capacity monitoring platform to track real-time usage of underlying cloud infrastructure services. When usage exceeds predefined thresholds, the monitoring platform issues alerts to notify relevant teams to take appropriate actions, ensuring the stable operation of products |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | and services. |

## 7.5 System Development and Change Management

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| E1 | System development and change management | Establish formal change management procedures and implement effective controls over system modification, production deployment and system fallback. In particular, obtain written management approval for both scheduled and emergency changes/fixes. | Customers should establish a change management procedure and implement effective monitoring controls for system changes. All changes must be authorized prior to implementation.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established a set of product and configuration change management standards, clearly defining each step in the change process and the responsible parties to ensure that changes are properly approved and tested before deployment. Tencent Cloud also defines a dedicated emergency change management process, which requires appropriate approval before execution.<br><br>All types of program changes—including application and configuration file updates, operating system modifications, and database changes—must undergo business impact analysis and include a rollback plan prior to deployment. These changes must be approved by designated responsible personnel. Tencent Cloud's change release system enforces that only authorized personnel may execute change operations, and all change-related logs are retained and subject to regular audits. After deployment, Tencent Cloud operations team verifies and monitors the changes in the production environment and records the results.<br><br>For operational changes that may affect customers, Tencent Cloud will promptly issue change notifications through official channels such as the website and internal messaging |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | systems. |
| E2、E3、E4、E5、E6 | Secure Software Development | E2 Mandate the following security practices in the software development life cycle (SDLC) to allow early identification and remediation of security vulnerabilities prior to the launch of new systems or major system changes:<br>- Consider security requirements (e.g. user authentication and authorisation, session management, data integrity, audit logging) during the system design phase;<br>- Establish secure programming practices;<br>- Conduct source code review including peer review and automated source code scanning; and<br>- Conduct security testing prior to migration to production environment.<br>E3 Establish test cases to ensure all critical functions are properly tested before production deployment and perform post-implementation review to ensure the reliability of system after modification.<br>E4 Set up user acceptance testing (UAT) environments or equivalent to adequately test system modifications before system migration to production environment.<br>E5 Implement a control mechanism to mask sensitive information, e.g. clients' | Customers should establish and implement a comprehensive project lifecycle management methodology to define processes for critical system development, testing, acceptance, implementation, and operations. This includes identifying, developing, testing, and enforcing security requirements, as well as conducting quality reviews for major technology-related projects.<br>To support customers in managing the development of lifecycle, Tencent Cloud provides **Cloud Native Build (CNB)** developer tools. CNB is based on the Docker ecosystem and abstracts environments, caches, and plugins using declarative syntax, enabling developers to build software more efficiently. CNB offers a complete developer toolchain with capabilities such as code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and custom task sets, effectively supporting the entire process from requirements to deployment and enabling agile development management.<br>**Penetration Testing Services (PTS)** can simulate large-scale customer business scenarios to comprehensively validate system availability and stability. It supports on-demand initiation of performance testing tasks and can generate traffic from multiple regions with millions of concurrent requests. PTS offers features such as traffic recording, scenario orchestration, traffic customization, and advanced scripting, enabling customers to quickly define test scenarios based on business models and accurately replicate large-scale application access patterns. This helps customers proactively identify performance issues in their applications.<br>Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | personal information, for system testing purposes.<br><br>E6 Conduct stress/performance testing with sufficient data volume to simulate the anticipated and historical peaks on the internet trading system and underlying technology infrastructure before production deployment. | Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls throughout the product lifecycle. Key security measures include:<br>• Security Training: Developers receive secure coding training and are required to follow secure coding guidelines.<br>• Requirements Analysis: Engage in discussions on business content, workflows, and technical frameworks to identify optimal security integration points.<br>• System Design: Perform threat modeling and security assessments of the chosen architecture.<br>• System Development: Provide Tencent-designed secure development components and enforce secure coding practices.<br>• Security Validation: Conduct code security checks, asset scans, web vulnerability scans, manual security assessments, penetration testing, and code audits to identify vulnerabilities.<br>• Release: Systems are deployed to production only after final security review and approval to prevent vulnerabilities from entering the live environment.<br>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. |

## 7.6 Cybersecurity Risk Assessment, Cyber-Attack Simulation and Incident Response

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| F1、F2 | Cybersecurity Risk Assessment, Network Attack Simulation Testing | F1 Carry out simulations of real-life cyber-attack scenarios to validate the effectiveness of the cyber defense mechanisms.<br>F2 Conduct regular independent assessments (e.g. IT audit, cybersecurity risk assessment, security penetration testing, and cyber-attack simulation on at least an annual basis) of Internet-facing and internal systems and underlying technology infrastructure, people and processes by qualified professionals. | Customers should regularly engage professionals to conduct cybersecurity exercises such as simulated cyberattacks, security assessments, and penetration testing.<br><br>Penetration Testing Services (PTS) simulate attack techniques and vulnerability discovery methods that hackers might use. These services employ controlled and non-destructive approaches to deeply probe the security of target systems, identify weaknesses in systems and network devices, and provide security hardening recommendations to help customers enhance system security. PTS can also be flexibly integrated into customers' product development, application deployment, and internal security validation plans.<br><br>To support customers in meeting regulatory requirements, Tencent Cloud has established an internal mechanism for regular vulnerability scanning and penetration testing. Vulnerability scans typically cover web vulnerabilities, component vulnerabilities, and configuration issues. Scanning tasks are automatically generated by the vulnerability scanning system to assess assets in the cloud environment, with identified vulnerabilities analysed, categorized, and remediated.<br><br>For penetration testing, the Tencent Cloud Security Team conducts full-chain, large-scale penetration tests on a regular basis, and performs targeted tests before new product launches or major changes. Test results are communicated via security tickets to relevant departments, which are responsible for timely remediation or implementing compensating controls to ensure that exploitable vulnerabilities identified during testing are properly addressed.<br><br>Tencent Cloud also conducts red-blue team exercises to simulate real-world cyberattack defence scenarios. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | The Tencent Cloud Security Team performs 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. Additionally, Tencent Cloud undergoes annual independent third-party audits, and provides attestation-based 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. |
| F3 | Incident Management | Arrange post-mortem review to be performed by independent functions or external professionals in the event of material security incidents, including system delays and system failures. | Customers should assign independent functions or professionals to conduct post-incident analysis and review following security events.<br><br>To support regulatory compliance, Tencent Cloud has established an Information Security Incident Management Standard, including a response and handling mechanism. Security incidents are recorded via Tencent Cloud's internal security operations system. Upon detection, incidents are analyzed and classified based on their nature, data sensitivity, and impact scope, and relevant personnel are promptly notified for follow-up handling.<br><br>Tencent Cloud has a periodic incident analysis mechanism, conducting multi-dimensional reviews (e.g., incident type, frequency, impact scope, severity), and implements preventive measures based on root cause analysis to avoid recurrence. For major security incidents, Tencent Cloud forms a dedicated task force to produce a special analysis report for management review. |

## 7.7 Data Backup and Contingency Planning

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| G1、G2 | Data backup | G1 Encrypt all backup media containing confidential and sensitive data and where | Customers should establish a backup management mechanism to regularly back up confidential and sensitive data. Backup storage media should be |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | applicable protect such media physically (e.g. use of locked box for storage transportation) to ensure secure storage and transportation between locations.<br>G2 Perform restoration test of data backup on a regular basis to ensure effectiveness of data recovery. | encrypted and physically protected, and backup recovery tests should be conducted periodically.<br>Tencent Cloud currently operates three independent data centers in Hong Kong, each with separate power and network infrastructure, enabling customers to store, process, and back up data locally within Hong Kong. Tencent Cloud offers multiple storage and database services with built-in backup capabilities to meet diverse customer needs, such as:<br>• **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.<br>• **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.<br>• **Cloud File Storage (CFS)**: Offers scheduled snapshot capabilities for flexible backup task configuration.<br>• **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.<br>• **TencentDB for MySQL**: Provides automatic and manual backup options, including cross-region backup, enhancing disaster recovery and data reliability.<br>• **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. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| G3、G4 | Disaster Recovery | G3 Establish a disaster recovery/secondary site to continue internet trading services or make alternative arrangements in the event of primary site outage with a view to minimizing disruption of internet trading services provided to clients.<br>G4 Conduct disaster recovery drill at least annually and update the disaster recovery plan where appropriate. | Customers should also establish disaster recovery or backup data centers, and formulate disaster recovery plans that are regularly tested and updated.<br><br>Tencent Cloud offers a wide range of products designed with high availability features to help customers achieve system and service resilience. For example:<br><br>• **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.<br><br>• **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.<br><br>• **Cloud Object Storage (COS)** provides cross-architecture, multi-device redundant storage, enabling disaster recovery and resource isolation for customer data to ensure durability.<br><br>• **TencentDB for MySQL** supports high reliability and availability with robust automatic backup and lossless recovery mechanisms.<br><br>• **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.<br><br>To meet regulatory requirements, Tencent Cloud |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | 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. |

## 7.8 Vendor management

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| H1、H2、H3 | Vendor Management | H1 Evaluate the cybersecurity resiliency of prospective vendors before onboarding.<br>H2 Include in the service level agreement with vendors (and/or intra-group entities) the following cybersecurity requirements, among others:<br>- compliance with company cybersecurity policies;<br>- escalation of security incidents;<br>- removal/destruction of data stored at vendors' systems and backups in the event of contract termination or deemed necessary; and<br>- reasonable indemnification or liability provisions.<br>H3 Conduct cybersecurity risk assessment and on-site audit of vendors, or review of auditor report of vendors, on a regular basis and require vendors to take remedial actions upon the identification of material deficiencies. | Customers should assess the cybersecurity capabilities of vendors prior to establishing business relationships, incorporate cybersecurity requirements into service agreements, and conduct regular cybersecurity risk assessments or review vendors' audit reports.<br>To support customers in meeting regulatory requirements, Tencent Cloud strictly complies with the laws and regulations of the jurisdictions in which it operates and has established procedures to ensure that its information security practices meet applicable legal, regulatory, and industry standards. While securing the underlying cloud infrastructure, Tencent Cloud also empowers customers by offering a comprehensive suite of cloud security features, tools, and controls to jointly build a robust and resilient cloud security framework.<br>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 scope and quality of services, protection of user data and intellectual property, audit and inspection rights, dispute resolution, termination and early exit provisions, confidentiality obligations, incident and change notifications, and the respective security responsibilities of both Tencent Cloud and its customers.<br>In addition, Tencent Cloud undergoes regular independent third-party audits and publishes |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | System and Organization Controls (SOC) reports to provide assurance on its internal control environment to cloud users, independent auditors, regulators, shareholders, and other stakeholders.<br><br>Based on actual circumstances and contractual agreements, Tencent Cloud will cooperate with customers' third-party security audits and oversight activities, providing dedicated support personnel and actively responding to customer-initiated audit requests. Furthermore, to support regulatory inspections by financial authorities, Tencent Cloud will promptly respond and provide necessary assistance in accordance with customer requirements. |

## 7.9 Raising Cybersecurity Awareness of Internal System Users

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| I1、I2 | Cybersecurity Awareness | I1 Provide structured cybersecurity awareness training to internal system users, including regular courses for new joiners, refresher courses and ad-hoc courses on a needs basis, explaining the company's cybersecurity-related policies and procedures and providing practical guidance to staff on how to implement these policies and procedures.<br>I2 Evaluate staff's understanding and compliance with company policies on IT risk and cybersecurity on a regular basis, with short tests, reminder prompts and phishing attack simulation as part of evaluation process. | Customers should establish a cybersecurity awareness training mechanism and conduct regular training sessions for internal system users. To support customers in meeting regulatory requirements, Tencent Cloud has implemented a comprehensive Information Security Training Program. This program requires participation from full-time employees, consultants, interns, and outsourced personnel. Training offerings include mandatory courses for all staff, specialized training for key roles, and elective professional modules. Topics covered include basic security awareness, office security, vulnerability identification and mitigation, privacy protection, incident response, secure development practices, and data security requirements.<br>Certain training sessions include security assessments, and employees must pass these assessments to be considered as having completed the course. This ensures that staff are familiar with Tencent Cloud's internal cybersecurity policies and requirements. |

# 08 How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Circular to all Licensed Corporations on Internet Trading and Information Technology Management

In addition to the circulars and guidelines mentioned in the previous sections, the SFC has also issued the following circulars:

- Circular to all Licensed Corporations on Internet Trading: All licensed corporations that provide internet trading services to customers must regularly conduct self-assessments of their internet trading systems, network infrastructure, related policies, procedures, and practices to ensure compliance with relevant electronic trading requirements. The SFC has developed an Internet Trading Self-Assessment Checklist to guide licensed corporations in performing these assessments.
- Circular to All Licensed Corporations on Information Technology Management: The management of licensed corporations should regularly review existing information systems, policies, and practices, and consider improvements where necessary to prevent unauthorized tampering or intrusion into information systems or related data.

These two circulars provide guidance on managing information technology for licensed corporations. The requirements primarily focus on areas such as information security policies, access control management, network security, encryption, system development and change management, user activity monitoring, data backup and business continuity planning, and vendor management. The corresponding requirements for cloud service providers are largely consistent with those described in Section 5 to 7 of this guide.

In this section, Tencent Cloud summarizes the control areas related to cloud service providers as outlined in the above circulars and briefly explains how Tencent Cloud, as a cloud service provider, assists licensed corporations in meeting these requirements.

For more detailed explanations and product information regarding Tencent Cloud's approach to these areas, please refer to the "Tencent Cloud's Response" sections in Section 5 to 7 of this document.

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| A. Information security policy (1-3、5) | 1 Management Oversight (3、6) | Establish and implement appropriate internal information security policy and perform regular review and consider enhancement where needed and raise staff awareness on the importance of information security | Customers should establish and implement necessary information security policies, review and update these policies regularly, and provide employees with information security awareness training.<br>Tencent Cloud has developed an information security management policy comprising an overarching security strategy, organizational structure, and security management framework. This policy effectively supports the secure operation and risk management of the cloud platform and guides the daily work and management processes of all departments and employees. Tencent Cloud's information security policy is reviewed annually to ensure that the objectives, procedures, and controls of the cloud |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby guaranteeing the adequacy and effectiveness of the policy. Employees can access these policies through Tencent Cloud's internal platform. |
| B.1 User account and access rights management (1-6)<br>B.2 Password policy and control (1-2)<br>B.3 Network and system access control (1-3) | 2 User Access Controls (3-5) | B1 User-account provisioning and access approval controls shall be implemented. Authorizations must be granted on a need-to-know basis, accounts must be reviewed regularly, and unnecessary user accounts and permissions must be removed promptly.<br>B2 Implement effective password policy and authentication mechanism.<br>B3 Ensure that only authorized personnel are granted access to both the testing and production environments. Remote access rights to external parties should be granted only when necessary and terminated immediately when no longer required. | Customers should establish identity authentication and access control mechanisms, implement effective password policies, and grant account permissions based on the principle of least privilege through proper approval processes. Regular account reviews should be conducted, and unnecessary account permissions should be promptly removed. Remote access authorizations should be strictly controlled and terminated immediately when remote connections are no longer required.<br>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.<br>Tencent Cloud has established an access control authorization policy and a privilege separation matrix mechanism, requiring user accounts to use unique identifiers. Password policies for employee accounts are set according to security baselines, covering aspects such as password length, complexity, lockout, and reset procedures. Tencent Cloud uses a Zero Trust security |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | management system to authenticate employee access, and users must complete multi-factor authentication before accessing internal resources.<br><br>Tencent Cloud maintains records mapping job roles to identity information and corresponding permission levels across business systems and conducts regular access reviews. In the production environment, Tencent Cloud has fully deployed bastion hosts to centrally manage administrator account permissions for backend system components. Operations personnel must access the production environment containing customer data through bastion hosts, and all operations accounts are equipped with multi-factor authentication. Backend maintenance operations are logged and stored centrally on a logging platform, and Tencent Cloud's internal audit team regularly reviews these logs.<br><br>For more details on identity authentication and access control, please refer to Section "7.3 System Access Monitoring Measures and Data Protection." |
| B.3 Network and system access control (4) | 3 Network infrastructure Architecture Design (4-7) | Avoid access to/by external network such as Internet unless proper network safeguards are implemented | Customers should implement network security measures—such as deploying network security devices and antivirus mechanisms—to mitigate risks associated with external network connections.<br><br>Tencent Cloud provides multiple services to help customers effectively manage network security, including **Cloud Firewall (CFW)**, **Web Application Firewall (WAF)**, and **Anti-DDoS**.<br><br>Tencent Cloud has deployed a mature network security architecture incorporating multiple layers of protection, such as firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS mitigation, network segmentation, and web application security. These mechanisms enable timely detection, filtering, and blocking of |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | malicious traffic to safeguard Tencent Cloud's network infrastructure. Tencent Cloud has established standardized network security configuration and baseline standards to ensure consistent security management across network devices, firewalls, operating systems, databases, and application systems.<br><br>The Tencent Cloud security team regularly reviews security policies and parameter settings for network devices such as routers, firewalls, and servers to ensure their effectiveness. Additionally, Tencent Cloud operates an internal network monitoring system to track and alert on these devices and uses a ticketing system to follow up and resolve identified security issues.<br><br>For more details on network infrastructure security, please refer to Section "7.2 Secure System and Network Infrastructure." |
| C. Encryption (1) | 4 Application Controls and Processing Integrity (10) | Apply data encryption to protect sensitive information transmitted outside secured internal network or stored in portable storage devices without strong physical/logical protection | Customers should establish an encryption management mechanism to ensure that sensitive data is encrypted during both storage and transmission.<br><br>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.<br><br>Tencent Cloud has established a comprehensive data management framework, strictly adhering to the principle of "data confidentiality." When storing data, Tencent Cloud uses multi-replica redundant storage and erasure coding technology and immediately takes necessary recovery measures upon detecting integrity errors, thereby |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | enhancing data fault tolerance. Customer data is encrypted using strong encryption algorithms to ensure data security. Communications on the Tencent Cloud console are protected by HTTPS encryption protocols.<br><br>For more details on data protection and encryption, please refer to Section "6.1 Protecting Customers' Internet Trading Accounts" and "7.3 System Access Monitoring Measures and Data Protection". |
| D. Change management (1-4) | 5 System implementation, Upgrade and Modification (2-3、5、9) | Test system changes properly, Maintain proper audit trails for system changes and test results. Seek approval from management before system changes are migrated to the production environment.<br>Test system capacity and performance with sufficient data and transactions volume with reference to anticipated and historical peaks | Customers should establish change management procedures to test system changes and properly retain test results. All changes must be authorized before implementation. In addition, customers should simulate the expected and historical peak traffic of internet trading systems and related infrastructure prior to deployment.<br><br>**In terms of change management**, Tencent Cloud has established a set of standards for managing product and configuration changes, clearly defining each step in the change process and the responsible parties to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud's change release system enforces that change operations can only be performed by authorized personnel and retains change-related logs for regular review. After deployment, Tencent Cloud monitors changes in the production environment and records the results.<br><br>**For capacity management**, Tencent Cloud forecasts capacity requirements based on business needs and formulates an annual capacity management plan. Using an internal capacity monitoring platform, capacity managers monitor usage in real time and identify usage trends.<br><br>For more details on system change management, please refer to Section "7.5 System Development and Change Management." |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | Customers should establish measures to protect test data and ensure that real data containing personal sensitive information is not used for system testing.<br><br>To assist customers in managing the application system lifecycle, Tencent Cloud provides **Cloud Native Build (CNB)** developer tools. CNB is based on the Docker ecosystem and abstracts environments, caches, and plugins using declarative syntax to help developers build software more efficiently. CNB offers a complete developer tool chain, including code hosting, high-performance CI/CD pipelines, AI-powered code review, cloud-based development environments, artifact management, and customizable task sets. These capabilities enable full lifecycle support from requirements to deployment and facilitate agile development management.<br><br>Tencent Cloud has established a comprehensive set of secure development standards for information systems, specifying security control measures for each stage of the project development process, including requirements analysis, system design, code security, testing, and release. Security and privacy protection principles are embedded throughout all phases of product development to ensure that cloud products receive adequate security controls throughout their lifecycle.<br><br>To guarantee end-user security, Tencent Cloud strictly follows the Secure Development Lifecycle (SDL) methodology when developing cloud platforms and products, aiming to integrate information security into the entire software development lifecycle. In addition, 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 |
| D. Change management (5) | 5 System implementation, Upgrade and Modification (1、6-8) | Avoid possible misuse of sensitive information by only allowing testing data to be used in testing environment | |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | development/testing environment.<br><br>For more details on secure system development, please refer to Section "7.5 System Development and Change Management." |
| E. User activities monitoring (1-3) | 7 Monitoring (1) | Make sure audit log is available to log user activities in the information systems and audit log should be restricted from modification.<br>Perform performance monitoring on a continuous basis to ensure the availability of information systems. | Customers should establish a system log collection and audit mechanism to monitor user activities within the system, the usage of sensitive applications and databases, and overall system performance. Audit records must be protected and must not be altered.<br><br>Tencent Cloud provides **Cloud Log Service (CLS)** to help customers address issues related to business operations, security monitoring, log auditing, and log analysis. CLS adopts a highly available distributed architecture and stores log data with multiple redundant backups to prevent data loss in case of single-node failures, ensuring high availability and reliability.<br><br>Through **CloudAudit**, customers can record logs, continuously monitor, and retain account activity related to operations across Tencent Cloud's infrastructure. Customers can also use **Elasticsearch Service (ES)** to aggregate and transmit 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 storage, search, and analysis.<br><br>Tencent Cloud uses Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage all server endpoints across the network. It tracks operator login activities, operational actions, and system anomalies such as OS errors or hardware failures, recording all events in logs. Leveraging years of experience and a robust rule base in security monitoring, Tencent Cloud's automated audit tools can promptly identify abnormal behaviours and trigger real-time alerts. |

| No. & Domain<br>Information Technology Management | Circular on Internet Transactions | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | For more details on log management, please refer to Section "7.4 Security Monitoring and Capacity Management." |
| F. Data backup and continuity planning (1-6) | 6 Backup and Contingency (1-15) | Perform backup on critical data on a regular basis. Test restoration of data from data backup.<br>Implement an effective business continuity plan. Based on the business continuity plan, IT disaster recovery plan should be formulated to ensure critical information systems can be resumed to support business operations. | Customers should establish a backup management mechanism to back up confidential and sensitive data, ensure that backup data is protected and accessible only to authorized personnel, and conduct regular backup recovery tests. In addition, customers should develop a disaster recovery plan and perform regular testing and updates.<br>Tencent Cloud ensures complete isolation between different regions to maximize stability and fault tolerance. To guarantee high data availability, each region is further divided into multiple isolated availability zones. This multi-zone design effectively reduces the impact of single-point failures, ensuring isolation between zones and supporting customers' business continuity.<br>Tencent Cloud's various storage and database services provide built-in backup capabilities to meet diverse requirements such as multi-redundant backups and cross-region disaster recovery. To help customers quickly respond and restore critical functions after a cybersecurity incident, Tencent Cloud offers products with high availability features to ensure system and service resilience. Tencent Cloud also develops detailed disaster recovery plans for its cloud products and conducts regular drills to ensure timeliness and feasibility.<br>Furthermore, Tencent Cloud has established a comprehensive business continuity and disaster recovery management system and has obtained ISO/IEC 22301 certification for Business Continuity Management Systems.<br>For more details on data backup and business continuity management, please refer to Section |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | "7.7 Data Backup and Contingency Planning." |
| \ | 8 Vendor Management (4-5) | Contracts concluded between the Internet trading system and its supporting infrastructure and external vendors and/or intra-group companies shall include service-level agreements that set out the contractual rights of data ownership (e.g., rapid deletion or destruction of data stored on the vendor's systems and backup media upon contract termination). | Customers should evaluate the services and performance of internet trading system and infrastructure providers when selecting vendors, and sign contracts and Service Level Agreements (SLAs) that clearly specify the customer's ownership of data.<br><br>Tencent Cloud provides online legal documents such as Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement, which clearly define the scope of Tencent Cloud's services and service levels, 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 matters. Customers may also negotiate to include additional requirements in separate agreements.<br><br>If customers need to terminate the contract due to business changes or future IT planning, they can back up and migrate cloud data and production environments at any time. Tencent Cloud supports data backup and migration using standard formats, and customers can use the same transmission methods and protocols as during cloud onboarding, or leverage network services such as **Direct Connect (DC)** and **VPN Connection** to ensure secure and reliable data migration during offboarding. After the termination of cloud services, Tencent Cloud follows strict data erasure procedures to completely delete customer data before reusing any previously purchased computing and storage resources.<br><br>For more details on vendor management, please refer to Section "7.8 Vendor Management." |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | |
| | | | Customers should conduct security penetration testing on internet trading systems and their infrastructure, or when significant changes occur, implement remediation measures based on test results, and report findings to management. In addition, customers should test patches before deployment.<br><br>Tencent Cloud's **Vulnerability Scanning Service (VSS)** leverages Tencent's extensive security experience and threat intelligence to maintain a comprehensive vulnerability rule base and provides professional, efficient detection capabilities for 0Day, 1Day, and NDay vulnerabilities. VSS enables regular security scans, continuous risk alerts, and vulnerability detection for customer assets, offering expert remediation recommendations to reduce security risks.<br><br>Tencent Cloud's **Cloud Pressure Testing (PTS)** simulates hacker techniques and vulnerability discovery methods in a controlled, non-destructive manner to thoroughly assess system security, identify weaknesses in targets and network devices, and provide hardening recommendations to improve system security.<br><br>Tencent Cloud has established regular vulnerability scanning and penetration testing mechanisms. Internal vulnerability scans typically include web vulnerabilities, component vulnerabilities, and configuration checks. Scanning tasks are generated periodically to assess assets in the cloud environment, and identified vulnerabilities are analysed, categorized, and remediated. For penetration testing, Tencent Cloud's security team conducts large-scale full-chain penetration tests regularly and performs targeted tests before new product launches or major changes. Test results are communicated via security tickets to responsible departments, which promptly patch |
| \ | 9 Application Vulnerability Management and Client Awareness Controls (1-5) | Conduct security penetration tests on the Internet trading system and its supporting infrastructure, or on any recent material changes, and follow up the test results to ensure that necessary remedial actions are taken. | |

| No. & Domain | | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| Information Technology Management | Circular on Internet Transactions | | vulnerabilities or implement compensating controls to ensure proper remediation.<br><br>Tencent Cloud regularly conducts red-team/blue-team exercises simulating 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. |

09

# How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Use of Generative AI Language Models

With the expansion of generative AI language models (AI language models) into the public domain, the SFC encourages and supports licensed corporations to use AI and AI language models responsibly to innovate and deliver products or services more effectively, or to enhance operational efficiency. However, AI language models may amplify existing risks and introduce additional risks beyond the scope of traditional AI. To promote responsible adoption of AI language models within the industry, the SFC issued the circular Use of Generative AI Language Models in November 2024, requiring licensed corporations to consider risk factors associated with AI language model use cases—such as hallucination risk, cyberattack risk, and service disruption risks when using external providers—and to implement appropriate risk mitigation measures.

When complying with this circular, Tencent Cloud, as a service provider of generative AI language model products, may be involved in certain activities related to regulatory requirements. This section explains how Tencent Cloud helps licensed corporations meet relevant requirements under clauses 20–29 of the circular, which address cybersecurity, data risk management, and third-party provider risks.

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.

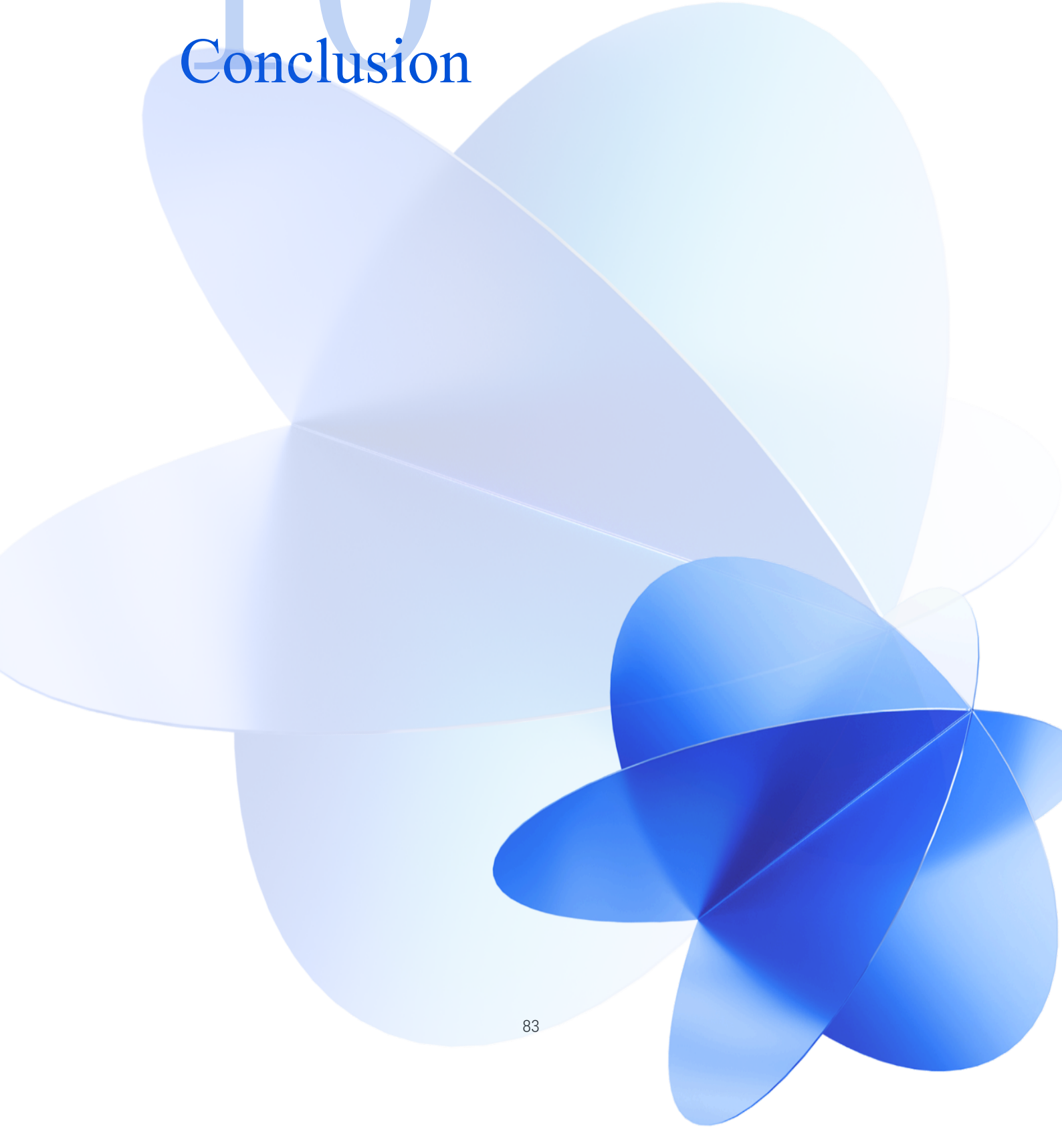
In operational governance, Tencent Cloud monitors, prevents, and responds to risks on an ongoing basis, implementing multi-layered security protections to ensure safe and accurate model outputs. We apply content tagging technologies to track risky content and continuously enhance model security, reinforcing 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.
  - Video Moderation (VM): Detects explicit or non-compliant video content to reduce manual review costs.
  - 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.

# 10 Conclusion



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

This guide is based on key regulatory requirements from Hong Kong Securities and Futures Commission (SFC) 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 SFC compliance standards, while also achieving efficient digital upgrades and innovative business development.

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

# 13 Version History

| Date | Version | Detail |
| --- | --- | --- |
| April 2026 | V1.0 | Initial Release |
| | | |