Tencent Cloud

# Tencent Cloud User Guide to Cyber Security Regulations & Guidelines in Singapore

April 2026

CONTENTS

# 01 Overview

Stable operation of digital services relies heavily on the continuous availability and proper functioning of foundational infrastructure such as cloud services and data centers. In February 2025, the Infocomm Media Development Authority (IMDA) of Singapore issued consultation guidelines on Resilience and Security of Cloud Services and Resilience and Security of Data Centres, recommending that all cloud service providers and data centers operators in Singapore adopt targeted measures to strengthen service resilience and security. These measures aim to minimize the risk of service disruptions and their potential impact on the economy and society.

The guidelines reference multiple international and industry standards, including Multi-Tier Cloud Security Standard (MTCS SS), Cloud Security Alliance Cloud Controls Matrix, ISO/IEC 27001, and ISO 22301, and outline best practices for mitigating risks associated with cloud services and data centers. These risks encompass both digital threats (such as misconfigurations and cyberattacks) and physical hazards (such as fire, water leakage, and cooling system failures).

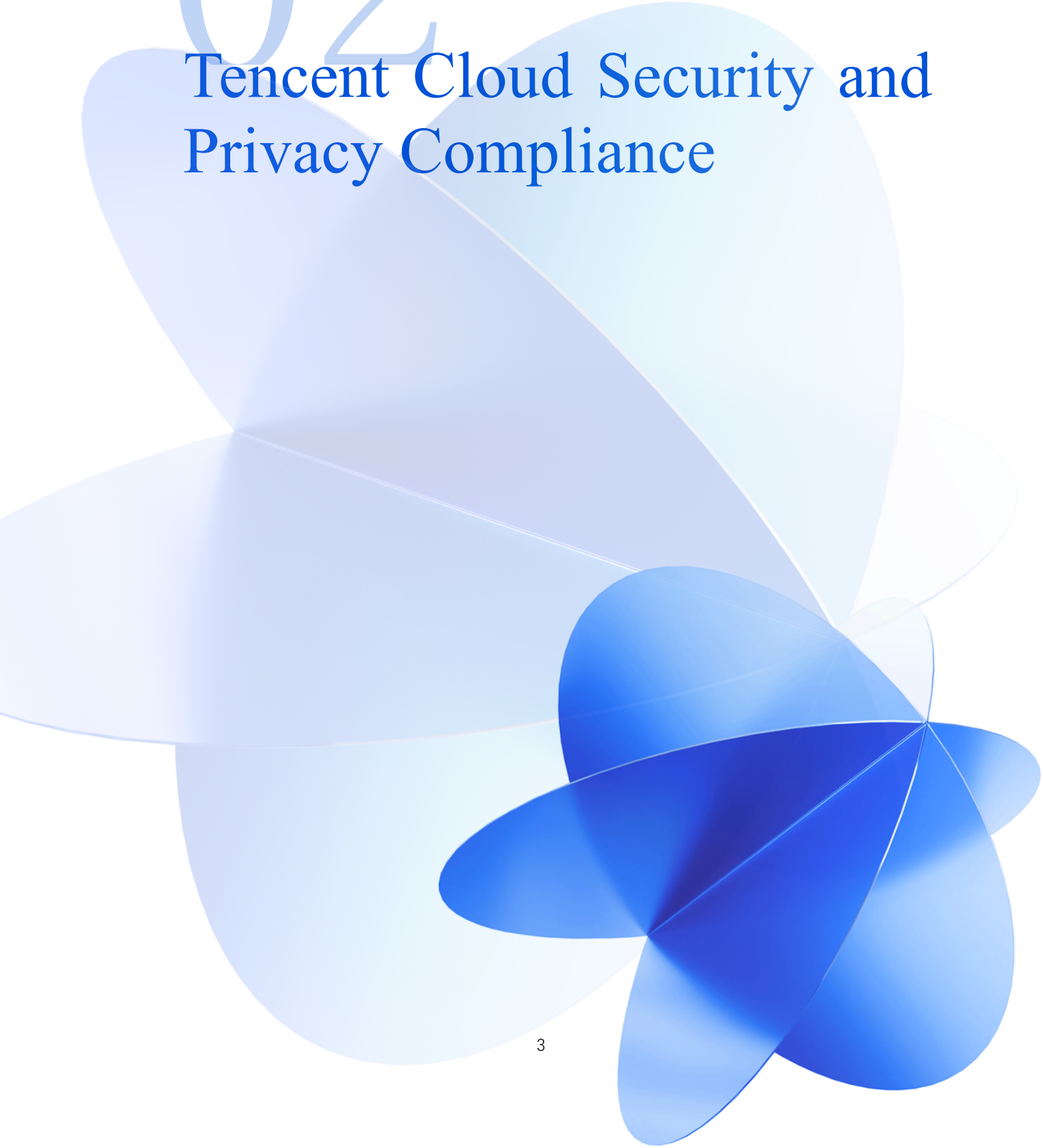
Key recommendations include implementing risk assessments, business impact analysis, business continuity planning, and cybersecurity safeguards.

Tencent Cloud closely monitors IMDA's regulatory developments and official publications and is committed to supporting customers in Singapore in meeting these compliance requirements. This document explains how Tencent Cloud aligns with the two consultation guidelines:

- Resilience and Security of Cloud Services
- Resilience and Security of Data Centres

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.<br><br>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 lifecycle 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. |

| | |
|---|---|
| | 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 |

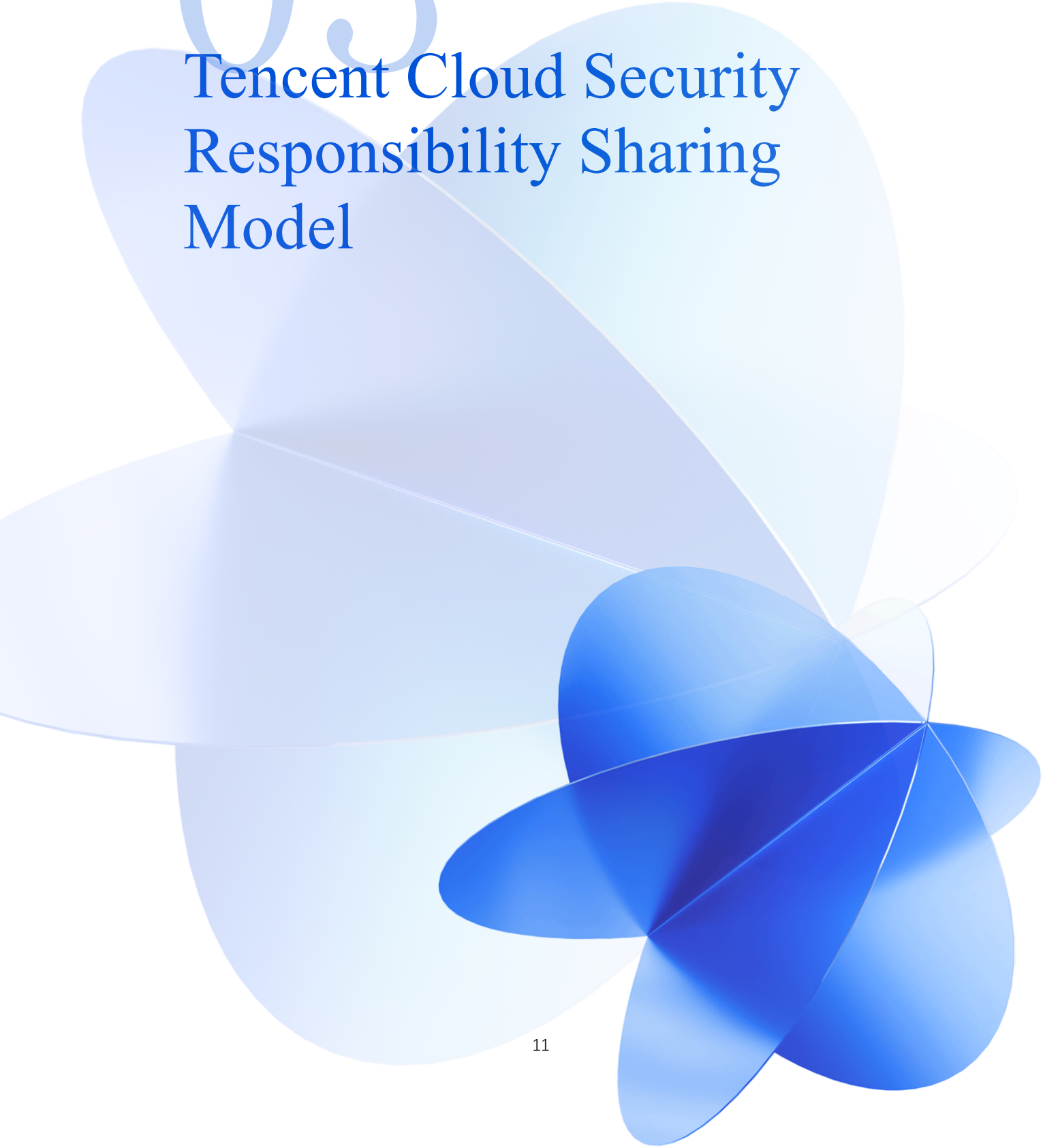
| | |
|---|---|
| | meet the stringent requirements for financial services in Singapore and Southeast Asia. |
| Data Protection Trustmark (DPTM) [Singapore] | The Data Protection Trustmark (DPTM) was developed by Singapore's Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA) to help organizations demonstrate responsible data protection practices.<br>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>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>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>Tencent Cloud demonstrates compliance through independent third-party audits, proving that the cloud services provided to financial customers in Malaysia strictly adhere to the regulatory requirements of the Malaysian financial industry. |
| IT compliance audit in Hong Kong Special Administrative Region (HKSAR) financial industry | The Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), and Insurance Authority (HKIA) have issued key regulatory requirements to govern the use of information technology by financial, insurance, and securities institutions.<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 obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure. |
| IT compliance audit in | Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange |

| | |
|---|---|
| Thailand financial industry | Commission (OSEC), the Office of Insurance Commission (OIC), and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers.<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<br>[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<br><br>[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><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><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><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><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.

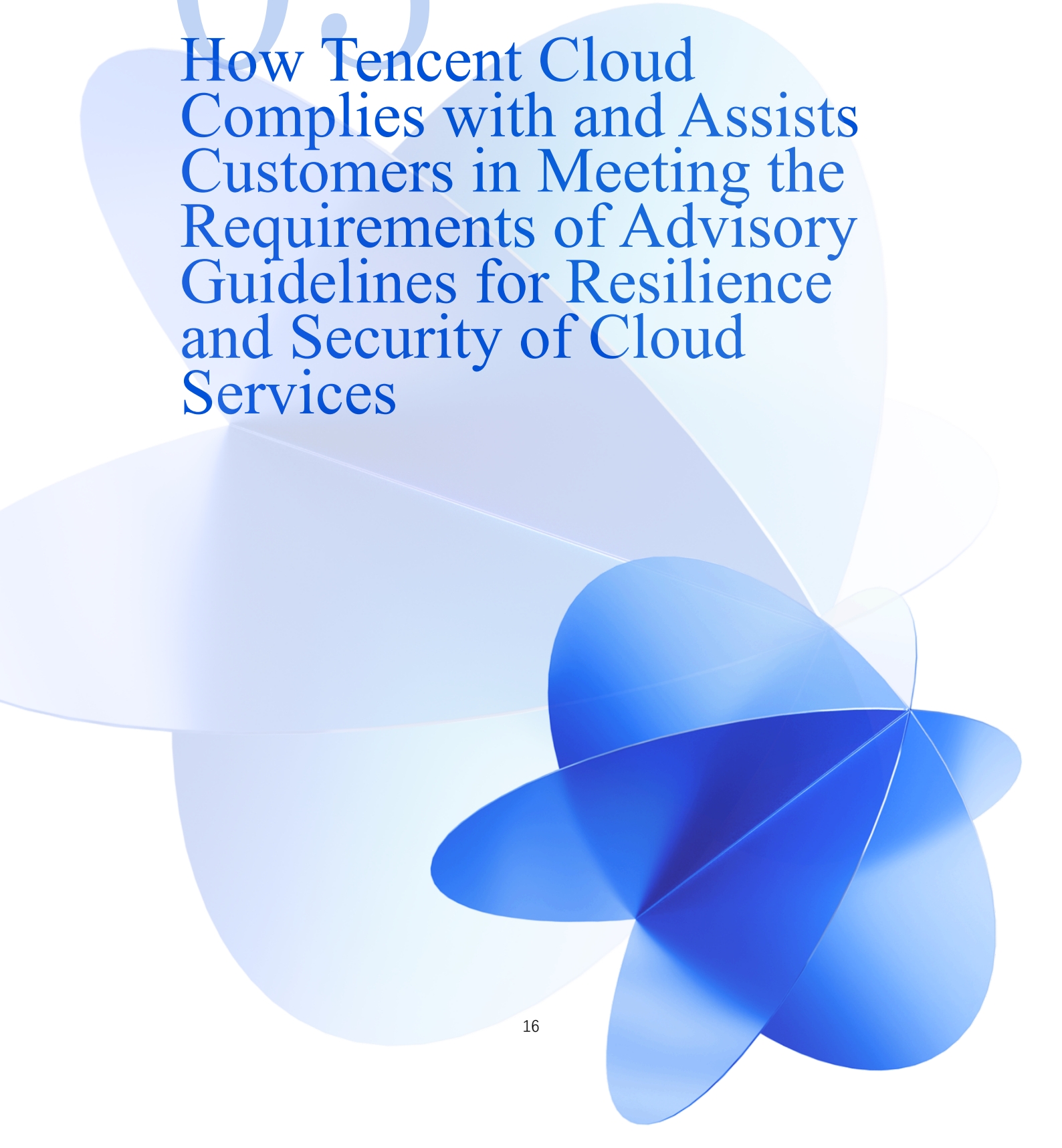
- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically 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 Complies with and Assists Customers in Meeting the Requirements of Advisory Guidelines for Resilience and Security of Cloud Services



Based on digital infrastructure—particularly cloud computing infrastructure such as cloud services and data centres—which has become a critical component of Singapore's economy, the Infocomm Media Development Authority (IMDA) issued the Advisory Guidelines for Resilience and Security of Cloud Services. These guidelines provide direction for Singapore cloud service providers (CSPs) on planning business continuity and managing resilience and security risks for cloud services.

The guidelines incorporate industry best practices and are voluntary in nature; however, IMDA strongly encourages CSPs to adopt them to enhance their resilience and security posture. The guidelines draw on IMDA's Multi-Tier Cloud Security Standard (MTCS), the Cloud Security Alliance Cloud Controls Matrix, and international standards such as ISO/IEC 27001. Control measures are organized into seven categories: Cloud Governance, Cloud Infrastructure Security, Cloud Operations Management, Cloud Service Management, Cloud Service Customer Access, Tenant and Customer Isolation, and Cloud Resilience.

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

## 5.1 Cloud Governance

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.2 | Information security management | CSPs should ensure that information security is managed within the CSP's overall administrative structure , , including:<br><br>a. establish information security roles, responsibilities, coordination, and information security policies and standards.<br><br>b. ensure Information Security Management System ("ISMS") for cloud computing has been developed, documented, approved and implemented.<br><br>c. provide oversight of its information security function.<br><br>d. ensure its management and board of directors are responsible for the management of information security;<br><br>e. establish and document an information security policy and | **In terms of information security management policies**, Tencent Cloud has established a comprehensive framework consisting of an overarching security strategy, organizational structure, and management system to ensure secure cloud platform operations and effective risk management. These policies undergo annual reviews to confirm that the objectives, procedures, and controls of the cloud security management system comply with relevant security strategies, standards, procedures, and legal requirements, ensuring adequacy and effectiveness.<br><br>Tencent Cloud has also implemented an Acceptable Use Policy, which clearly defines the responsibilities and obligations of employees and third parties when using Tencent Cloud resources (including but not limited to IT systems, networks, devices, and data). This policy regulates appropriate usage and mitigates potential risks.<br><br>Tencent Cloud is certified against internationally recognized standards, including:<br><br>• ISO/IEC 27001 – Information Security |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | baseline requirements;<br><br>f. ensure that the information security policy is reviewed and maintained up to date<br><br>g. ensure that auditable entities are established and updated periodically such as reviewing the scope of audit, determining the effectiveness of the audit scope, etc;<br><br>h. designate personnel as the primary and backup information security liaisons who minimally, are the points of contact with local authorities, and are contactable by the customers; and<br><br>i. establish and document an acceptable use policy for critical and new technologies, services and end-user devices in accordance with industry standards, and is communicated to all relevant employees and third parties. | Management System<br>• ISO/IEC 27017 – Cloud Service Information Security Management<br>• ISO/IEC 22301 – Business Continuity Management<br>• ISO/IEC 20000 – IT Service Management<br><br>**In terms of organizational structure**, Tencent Cloud has established a dedicated security governance framework, defining roles and responsibilities across different levels and setting mechanisms for security audits and risk assessments. Tencent has formed a Security Technology Committee and specialized security teams across various domains. Additionally, Tencent Cloud maintains robust HR management standards and procedures to ensure personnel are recruited and assigned according to role requirements.<br><br>Tencent Cloud brings together industry-leading security experts to deliver secure, reliable, professional, and compliant products and services. Regional Information Security Liaisons are appointed to maintain smooth communication with local regulators and customers, ensuring compliance with legislative, regulatory, and contractual obligations.<br><br>**In terms of security audits**, Tencent Cloud's security team conducts at least one internal security audit annually to ensure compliance with applicable laws, regulations, and security standards. Tencent Cloud also undergoes regular independent third-party audits and provides System and Organization Controls (SOC) reports to cloud customers, auditors, regulators, shareholders, and other stakeholders, demonstrating the effectiveness of internal controls.<br><br>Specifically for Singapore, Tencent Cloud has achieved MTCS Level 3 certification and Cyber Trust Mark, confirming that Tencent Cloud has implemented robust risk management mechanisms and delivers secure cloud services. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.3 | Information human resources | CSPs should ensure that all employees and third parties are suitable for their roles prior to employment or contract and that they understand their responsibilities, employment and contract terms and conditions (including termination) to reduce the risk of theft, fraud or misuse of facilities. CSPs should:<br><br>a. perform background checks in accordance with applicable ethics and contractual obligations;<br><br>b. evaluate personnel security (including third parties) at least annually;<br><br>c. ensure employees and relevant third parties minimally comply with organization's policies, and re-acknowledgement of acceptance of information security obligations agreement annually and prior to termination of service;<br><br>d. establish a formal disciplinary process ;<br><br>e. ensure all assets owned by the organization are duly accounted for and returned by employees and relevant third parties; and<br><br>f. establish, implement and review an information security training and awareness programme for employees and relevant third parties upon hire and at least annually. | Tencent has established comprehensive HR management standards and procedures to ensure personnel are selected, recruited, and assigned according to job requirements. Tencent Cloud has implemented a clear employee lifecycle management process, including onboarding, employment, and offboarding procedures.<br><br>**Before employment**, applicants undergo interviews to assess their suitability for the role. Based on applicable laws and job level, the HR department conducts background checks prior to hiring. These checks include verification of past employment history, criminal background, and academic qualifications. The results are recorded in Tencent Cloud's HR management system.<br><br>**Upon employment**, internal staff must sign an employment agreement and a confidentiality agreement. The employment agreement specifies Tencent Cloud's security policies and the responsibilities of employees or third-party personnel regarding information security and personal data protection. The confidentiality agreement outlines confidentiality obligations and penalties for violations. Outsourced staff are also subject to background checks and bound by employment and confidentiality requirements stipulated in agreements between Tencent Cloud and the outsourcing vendor. Legal teams review and update confidentiality requirements as needed.<br><br>Tencent Cloud provides a series of information security training and awareness programs to educate employees on security policies, procedures, and standards. Employees are required to participate in regular information security awareness training.<br><br>The **offboarding process** includes timely termination of user accounts and access rights, as well as retrieval of company assets. All physical assets are assigned to designated custodians and registered in Tencent Cloud's internal asset tracking system. A regular inventory check is conducted to verify asset existence and record results. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed. |
| 2.4 | Risk management | CSPs should establish and maintain a cloud-specific risk management programme to identify, quantify, prioritize, and mitigate or resolve risks impacting the cloud service operations and information assets. CSPs should:<br><br>a. establish and maintain a cloud-specific risk management programme that minimally include the process and methodology, risk identification/ assessment/ treatment/ mitigation plan and address residual risk at least on a quarterly basis;<br><br>b. conduct formal risk assessment at least annually or when there are significant changes;<br><br>c. establish a process to review and monitor risks to the cloud environment including the internal and external networks, hardware, software, applications, systems interfaces, operation and human elements; and<br><br>d. develop and maintain a risk register to monitor and report all | Tencent Cloud develops and maintains an internal risk management framework based on internationally recognized standards, including ISO/IEC 27001:2022, ISO/IEC 27018:2014, MTCS, and CSA STAR, to identify, analyze, and manage identified risks. The framework addresses both strategic and operational risks, covering security, availability, and confidentiality.<br><br>Tencent Cloud conducts formal risk assessments at least annually, referencing industry security incident reports, Tencent Cloud's accumulated practices, and professional risk databases to identify risks within Tencent Cloud's products and service processes. Each risk is evaluated based on asset value, likelihood of occurrence, and impact severity, resulting in a calculated risk level. Based on the analysis, Tencent Cloud defines mitigation strategies and implements measures to reduce risks to an acceptable level.<br><br>For identified risks, Tencent Cloud takes appropriate follow-up actions, records them, and continuously monitors risk treatment progress. Residual risks are assessed to ensure responsible parties manage risks in accordance with Tencent Cloud's risk management requirements. Tencent Cloud also maintains and updates risk assessment methodologies and risk registers based on industry trends and internal management practices.<br><br>Tencent Cloud communicates updates regarding product or service features, versions, and changes through announcements, email notifications, in-console messages on the Tencent Cloud website, or |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | identified risks. | other appropriate channels. |
| 2.5 | Third party | CSPs should ensure that it has an effective control framework over its third-party service providers supporting the cloud environment. CSPs should:<br><br>a. establish the framework that include third party service providers due diligence, agreement, delivery management, assurances over their performance and compliance with internal controls;<br><br>b. carry out due diligence to subcontracting services to third-party service provider(s);<br><br>c. develop and maintain risk management procedures, overseeing the risks and impact arising from third-party service;<br><br>d. ensure that written contractual agreements shall be made with every third-party service provider, which should also include contractual provisions to address relevant third-party risks;<br><br>e. ensure that the third-party service provider minimally has implemented all controls, service definitions and delivery levels as agreed in the third-party agreement, etc; and<br><br>f. (additional measure) ensure open-source components are safe to use, to protect against cyberattacks via software supply chain. | **In terms of vendor risk management**, Tencent Cloud has established a comprehensive vendor risk management program, which includes strict security assessments, regular monitoring, annual evaluations, independent reviews, and clearly defined outsourcing agreements.<br><br>Tencent Cloud enters into formal service agreements with its subcontractors that explicitly set out responsibilities and obligations relating to security, privacy protection, confidentiality, and compliance. In addition, Tencent Cloud continuously monitors subcontractors' service levels to ensure that sub-processing operations remain secure and stable. In accordance with the security and operational standards stipulated in the contracts, Tencent Cloud regularly assesses subcontractors' delivery performance and takes appropriate remedial action for any issues identified, thereby ensuring that their deliverables meet the agreed security and quality requirements.<br><br>**In terms of third-party product management,** Tencent Cloud has implemented supply chain security requirements for external components. Before introducing third-party components, Tencent Cloud conducts security admission reviews and applies hardening measures to ensure products pass pre-launch security checks. Post-launch, Tencent Cloud performs ongoing security operations and inspections, promptly addressing vulnerabilities. Security performance evaluations are conducted to identify risks, drive supplier improvements, and review future cooperation strategies.<br><br>Tencent Cloud has established security management standards to ensure that all open-source components introduced by development teams come from trusted sources and undergo security reviews. This process guarantees that open-source components are used safely and legally. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.6 | Legal and compliance | CSPs should ensure that they and their third-party service providers conform to the CSPs' information security and risk management policies, standards, and procedures and contractual obligations. CSPs should:<br><br>a. identify, create, maintain and review documentation minimally on compliance, cross-border and transit requirements, contractual requirements;<br><br>b. plan and conduct regular reviews to ensure that all information security and risk management procedures are complied with, in accordance with its organizational policies and standards;<br><br>c. establish procedures, training or awareness, and relevant policy enforcement actions to deter or prevent employees from unauthorized access, and enforcement of commercial agreements with relevant third parties and end users with acceptable use policies or agreements;<br><br>d. use cryptographic controls that are compliant to relevant agreements, applicable laws and regulations, etc.;<br><br>e. ensure the third-party service providers providing relevant services demonstrate compliance with the relevant policies, agreements and requirements; and | **In terms of compliance**, Tencent Cloud strictly adheres to the laws and regulations of the jurisdictions in which it operates and has established security compliance procedures to ensure that information security operations meet applicable legal, regulatory, and industry standards. Tencent Cloud's legal team continuously identifies and collects compliance requirements relevant to its business, maintains a comprehensive regulatory inventory, and updates it regularly.<br><br>**In terms of audits and reviews**, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture and ensure compliance with relevant laws, regulations, and security standards. Tencent Cloud also undergoes annual independent third-party audits globally, providing assurance reports such as System and Organization Controls (SOC) to cloud customers, auditors, regulators, shareholders, and other stakeholders. The Cloud Platform Security Center regularly evaluates adherence to security policies and processes, covering areas such as sensitive information leakage, vulnerability remediation, and secure configurations. Tencent Cloud conducts annual performance reviews and risk assessments of subcontractor services.<br><br>Tencent Cloud enforces security responsibilities and obligations through Acceptable Use Policies, service agreements, and third-party cooperation agreements. Tencent Cloud also requires internal employees and third-party service providers to undergo regular training to strengthen security and compliance awareness and ensure adherence to relevant policies and standards.<br><br>**In terms of supplier management**, Tencent Cloud also exercises effective control over its subcontractors through rigorous security assessment and onboarding, periodic monitoring and evaluation, and clearly defined outsourcing-service agreements. |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | f. provide a mechanism for customers to perform continuous or real-time compliance monitoring. | **In terms of encryption controls**, Tencent Cloud has implemented a key management mechanism to manage cryptographic keys throughout their lifecycle, ensuring confidentiality, integrity, and availability. Tencent Cloud uses internationally recognized encryption algorithms and products to encrypt data and keys.<br><br>Tencent Cloud provides cloud services in accordance with agreed Service Level Agreements (SLAs). Each SLA specifies performance metrics, measurement standards, and reporting requirements, which are published on the Tencent Cloud official website. Tencent Cloud continuously monitors service performance and availability and provides real-time monitoring through the management console. |
| 2.7 | Incident management | CSPs should implement incident management controls to ensure that information security events and weaknesses impacting the information assets and systems in the cloud environment are communicated in a timely manner. CSPs should:<br><br>a. implement and maintain an information security incident response plan and procedures to respond to security incidents;<br><br>b. ensure that the incident response plan is relevant and effective;<br><br>c. establish an information security incident reporting process; and<br><br>d. establish clear processes and procedures to handle problems arising from all incidents, including information security and non-information security | Tencent Cloud has established a comprehensive incident management framework, including reporting, response, and handling mechanisms with defined processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected and identified incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies the responsible personnel for follow-up and resolution.<br><br>Tencent is committed to building an active defense system based on the principles of "Intelligence–Attack & Defense–Management–Planning." By integrating threat intelligence, artificial intelligence, and big data technologies, Tencent enhances the efficiency and responsiveness of security incident handling. Tencent Cloud's response efforts focus on vulnerability detection, intrusion investigation, and attack prevention. The security operations team operates 24/7, enabling rapid intervention and alert handling, conducting preliminary analysis, and formulating containment strategies to prevent attacks or security incidents. For major security incidents, Tencent Cloud forms a dedicated task force to produce a detailed analysis report for senior |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | incidents. | management. |
| 2.8 | Data governance | CSPs should ensure that only authorized users have access to the data stored in the cloud environment at all times. CSPs should:<br><br>a. establish controls to secure data according to its classification and define handling procedures;<br><br>b. establish clear ownership of data;<br><br>c. ensure data integrity on input/output, transmission or exchange of data and data in storage at all times;<br><br>d. establish and implement procedures and controls for data labelling/handling requirements;<br><br>e. establish controls and procedures to protect data from loss and destruction by other tenants or by CSP authorized agents;<br><br>f. establish data storage and retention policies and procedures, and communicate these procedures to the customers;<br><br>g. establish and implement data backup procedure;<br><br>h. establish and implement secure disposal and decommissioning procedures for the hardcopy, media and equipment;<br><br>i. establish secure disposal verification procedures for live | **In terms of data classification and governance**, Tencent Cloud has established data security management procedures that define principles for data classification, categorization, and protection. Data owners are required to implement appropriate security measures throughout the data lifecycle—including collection, transmission, access control, backup, transaction protection, and third-party data exchange—based on classification requirements to ensure confidentiality, integrity, and availability. Customer data is classified as a high-security-level data within Tencent Cloud, and customers retain exclusive ownership and control over their data. Tencent Cloud employees will never access customer data unless explicitly authorized by the customer for service delivery or troubleshooting, or as required by law for criminal investigations. 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.<br><br>**In terms of data storage protection**, Tencent Cloud's storage and database products support encryption using strong, industry-standard algorithms and full lifecycle key management to ensure data confidentiality. Data is stored with multi-replica redundancy and erasure coding technology, enabling recovery measures when integrity errors are detected and significantly improving fault tolerance.<br><br>**In terms of data access protection**, Tencent Cloud has implemented access control management standards and established permission and authorization mechanisms. Bastion hosts are fully deployed in production environments to centrally manage administrator account privileges for backend system components. For multi-tenant isolation, Tencent Cloud adheres to the principle of "data privacy" through mechanisms such as virtualization layer access control policies, internal |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | instances/snapshots, dormant VMs and backups;<br><br>j. provide customers with a mechanism to track data; and<br><br>k. implement controls to prevent migration of production data to systems that do not have the same (or greater) level of controls. | private network isolation, web console permission allocation and authentication, session IDs and access keys, ensuring tenants cannot access, obtain, or tamper with other tenants' data. Tencent Cloud also provides customers with fine-grained access management capabilities for cloud products and resources.<br><br>**In terms of data transmission protection**, all communications on the Tencent Cloud console are encrypted using HTTPS. Tencent Cloud APIs also support HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level for customer workloads.<br><br>**In terms of data backup**, Tencent Cloud has established backup management procedures in compliance with legal requirements to back up critical data. Internal sensitive information is backed up according to classification-based strategies, with regular restoration tests. For customer data, Tencent Cloud provides multi-replica storage and backup services as part of its product offerings and assumes responsibility for backup services as defined in the Service Level Agreement (SLA).<br><br>**In terms of data deletion and destruction**, Tencent Cloud applies strict data erasure procedures. After the retention period expires, all customer data—including copies and backups—will be permanently deleted and rendered irrecoverable. If any media used to provide Tencent Cloud services becomes faulty or reaches end-of-life, Tencent Cloud will promptly perform complete physical destruction in accordance with rigorous internal processes. |

## 5.2 Cloud Infrastructure Security

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.9 | Audit logging and monitoring | CSPs should ensure that activities performed and events occurred in the cloud environment are being tracked | Tencent Cloud has established comprehensive standards and mechanisms for recording, extracting, storing, protecting, analyzing, and auditing logs, including login logs, operation logs, |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | and maintained for a period of time to detect any unauthorized activities and to facilitate investigation and resolution in the event of security incidents (e.g., access violations). CSPs should:<br><br>a. establish a process to track and monitor all access to network resources and system components;<br><br>b. establish a process to review logs;<br><br>c. ensure audit trails of all access to network resources and system components are captured and protected;<br><br>d. establish a log retention procedure; and<br><br>e. ensure integrity and accuracy of the usage logs at all times. | system logs, and security event logs. All logs are centralized and managed through Tencent Cloud's log management platform, with strict backup and protection measures to prevent unauthorized modification or deletion. Backup logs are retained for more than one year. Tencent Cloud uses automated security audit tools and internal audit teams to review logs, detect anomalies, and mitigate operational risks.<br><br>Tencent Cloud has fully deployed bastion hosts in its production environment to centrally manage administrator account permissions for backend system components. Internal operations personnel must obtain authorization before accessing the bastion host, and only designated Tencent Cloud operations staff are permitted access. Bastion host login requires multi-factor authentication. All operational records are stored in the centralized log platform and regularly reviewed by Tencent Cloud's internal audit team. |
| 2.10 | Secure configuration | CSPs should ensure that the systems in the cloud infrastructure and the supporting networks are designed and configured securely to prevent against unauthorized entry points or malicious activities through weak system configurations. CSPs should:<br><br>a. develop configuration standards for all system components and network device;<br><br>b. implement controls to prevent malicious code threats;<br><br>c. implement controls to | Tencent Cloud has established standardized configuration and baseline security standards for network devices, firewalls, host operating systems, databases, and application systems. Tencent Cloud uses scanning tools to check configurations of operating systems, database management systems, network devices, and virtual images, continuously detecting and correcting deviations from baseline standards. When a deviation is identified, the system automatically generates a security ticket and assigns it to the responsible department for timely remediation.<br><br>In terms of host security, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to monitor and manage all server endpoints across its network. The EDR solution supports antivirus and intrusion detection, security |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | address the risks associated with portable code;<br><br>d. implement controls for port protection;<br><br>e. restrict and tightly control the use of utility programmers;<br><br>f. implement controls to manage inactive sessions;<br><br>g. configure system security parameters to prevent misuse of services and protocols;<br><br>h. implement controls to restrict use of unapproved or unauthorized software;<br><br>i. perform compliance checks to ensure all security configurations are applied according to baseline standards. | baseline and vulnerability scanning, and compliance auditing for command operations and login activities. Alerts are triggered when malicious programs or abnormal behaviors are detected, and Tencent Cloud tracks and resolves these alerts through its ticketing system. Additionally, Tencent Cloud regularly reviews and updates EDR security policies, including user permission and system access policies. |
| 2.11 | Security testing and monitoring | CSPs should conduct security testing and implement monitoring controls across the cloud infrastructure including services, VMs and physical infrastructure to detect vulnerabilities and malware in a proactive and timely manner. CSPs should:<br><br>a. conduct internal and external vulnerability scans when there are significant changes in the infrastructure or at regular intervals;<br><br>b. conduct network layer and application layer penetration testing from the Internet, cloud service management network, and CSP internal network when there are significant | **In terms of Vulnerability Scanning and Penetration Testing**, Tencent Cloud has established a regular vulnerability scanning and penetration testing mechanism. Automated scanning tasks are scheduled through the vulnerability scanning system to assess assets within the cloud environment. Identified vulnerabilities are analyzed, categorized, and remediated promptly.<br><br>The Tencent Cloud Security Team conducts comprehensive end-to-end penetration tests on a regular basis and performs targeted penetration testing prior to new product launches or significant system changes. Test results are communicated via security tickets to the responsible departments, which are required to implement timely fixes or compensating controls to ensure that exploitable vulnerabilities are properly addressed. In addition, Tencent Cloud periodically organizes red team/blue team exercises to simulate real-world cyberattacks and |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | infrastructure changes, or application upgrades, or modifications, or at regular intervals; and<br><br>c. implement a security monitoring process, including implementing appropriate network intrusion detection or prevention systems to detect/deter abnormal network activities. | validate defensive capabilities.<br><br>**In terms of Network Monitoring and Defense**, Tencent Cloud operates an internal network monitoring system to continuously monitor routers, firewalls, and network servers. Alerts are generated for potential security issues, which are tracked and resolved through an integrated ticketing system. |
| 2.12 | System acquisition and development | CSPs should implement system acquisitions and development security controls to ensure that security is an integral part of the information systems as well as the business processes associated with these systems. CSPs should establish policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities. | **In terms of development security,** Tencent Cloud has also established internal secure development standards and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management, and ISO/IEC 9001 Quality Management standards throughout the product security development lifecycle. Security and privacy principles are embedded across all stages—requirements, design, development, testing, delivery, and operations—to ensure adequate security controls throughout the product lifecycle. Key security measures include:<br><br>• Security Training: Developers receive secure coding training and are required to follow secure coding guidelines.<br><br>• Requirements Analysis: Engage in discussions on business content, workflows, and technical frameworks to identify optimal security integration points.<br><br>• System Design: Perform threat modeling and security assessments of the chosen architecture.<br><br>• System Development: Provide Tencent-designed secure development components and enforce secure coding practices.<br><br>• Security Validation: Conduct code security checks, asset scans, web vulnerability scans, manual security assessments, penetration testing, and code audits to identify |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | vulnerabilities.<br>• Release: Only after all high-risk issues have been fixed can the system be released to the production environment.<br><br>**In terms of third-party product usage**, Tencent Cloud has established supply chain security management requirements. These requirements mandate security admission reviews before introducing external components, as well as security hardening and defense measures prior to launch to ensure products pass pre-launch security checks. After launch, Tencent Cloud performs continuous security operations and inspections, promptly addressing security issues. Tencent Cloud also evaluates the security performance of products to identify risks, drive supplier improvements, and reassess future cooperation strategies. |
| 2.13 | Encryption | CSPs should implement encryption and secure cryptographic key management to ensure that sensitive information in transmission or in storage electronically is being protected against unauthorized use or disclosure. CSPs should:<br><br>a. ensure that encryption policies and procedures are established and provide applicable encryption mechanisms.;<br><br>b. implement encryption on non-console administrative access, electronic commerce and online transactions (where applicable);<br><br>c. establish key management procedures to address all | **In terms of encryption and key management**, Tencent Cloud has established security management standards that define requirements for key application, generation, storage, usage, transmission, update, and destruction. All operations throughout the key lifecycle follow strict principles of dual control, secure handover, proper custody, and timely updates. During key usage, Tencent Cloud enforces segregation of duties, rigorous approval processes, and authenticated operations, while maintaining detailed key operation logs and conducting regular audits.<br><br>For cryptographic operations during data transmission and storage, Tencent Cloud requires internal teams to comply with internationally recognized cryptographic standards and regulations, using high-security algorithms such as AES-256 and ensuring key lengths meet security requirements.<br><br>**In terms of network communication security**, all customer communications on the Tencent Cloud console are encrypted using the HTTPS |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | components of the key management life cycle;<br><br>d. ensure that information involved in electronic messaging shall be appropriately protected. | protocol. Tencent Cloud APIs provide HTTPS encryption, signature verification, and status monitoring to ensure port-level communication security for customer workloads. To enable secure and fast access to cloud business systems anytime, anywhere, and from any mainstream device, Tencent Cloud also supports SSL VPN remote access technology.<br><br>Furthermore, Tencent Cloud deploys a Zero Trust Security Management System on employee office terminal (including laptops and workstations) to enforce endpoint control. This system supports sensitive data protection and audits outbound activities such as email, cloud storage, remote control, and file transfer tools, intercepting unauthorized data exfiltration and preventing sensitive data leaks. |

## 5.3 Cloud Operations Management

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.14 | Operations | CSPs should implement operations security controls to ensure that the operations of the cloud are documented, secure, reliable, resilient and recoverable. CSPs should:<br><br>a. establish operations management policies and procedures documentation for equipment maintenance and management of its cloud services' operations to ensure continuity and availability of its operations;<br><br>b. ensure proper and complete documentation and assessment of the service operations;<br><br>c. establish a process to monitor and plan capacity and resource requirements to | **In terms of operations management**, Tencent Cloud has established standardized procedures to guide daily operational activities for operations personnel. Tencent Cloud leverages mature, automated operations management platforms to manage operational tasks and strictly controls change windows through internal mechanisms, ensuring requests are completed within designated timeframes. Detailed operational security "red lines" are defined, and internal security reviews are conducted regularly. To ensure traceability and accountability in production environments, all backend operational activities are thoroughly logged, centralized in the log management platform, and periodically reviewed by Tencent Cloud's internal audit team to identify and investigate suspicious actions.<br><br>**In terms of capacity planning and management**, Tencent Cloud has implemented capacity management procedures that assign |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | ensure system and service performance;<br><br>d. state the service level and performance including subsequent changes in the contractual agreements or other means of communication acceptable to the customers;<br><br>e. establish a process to ensure reliability and resilience of storage systems and edge nodes supporting critical information assets either in a single facility or between multiple facilities;<br><br>f. establish a process to ensure recoverability of systems supporting critical information assets; and<br><br>g. (additional measure) implement processes to deal with reporting of vulnerabilities by researchers. | responsibility to business units for forecasting and planning system capacity. Tencent Cloud uses an internal monitoring platform to track real-time capacity utilization of underlying cloud services and identify usage trends. Business units then forecast capacity requirements based on historical trends and anticipated new business needs, ensuring continuity of operations and developing annual capacity management plans.<br><br>**In terms of service levels and performance**, Tencent Cloud delivers cloud services in accordance with Service Level Agreements (SLAs) defined for each product. SLAs specify performance metrics, measurement standards, and reporting requirements, all published on the Tencent Cloud official website. Service performance and availability are continuously monitored, and customers can access real-time metrics through the management console.<br><br>**In terms of resilience and recoverability**, Tencent Cloud requires cloud products to adopt multi-data-center redundancy within a single region to ensure business continuity. Detailed disaster recovery plans are established for cloud products and critical processes, and regular drills are conducted to validate timeliness and feasibility.<br><br>**In terms of vulnerability management**, Tencent Cloud has implemented threat and vulnerability management procedures and operates internal and external vulnerability reporting platforms. Tencent Cloud also runs a "Bug Bounty Program," inviting industry security experts to help identify system vulnerabilities and risks. All identified vulnerabilities are promptly tracked, analyzed, and remediated. |
| 2.15 | Change Management | CSPs should implement change management controls to ensure that changes to the cloud infrastructure are carried out in a planned and authorized | **In terms of change management,** Tencent Cloud has established a standardized framework for product and configuration change management, clearly defining each step in the change process and the corresponding responsible parties. This |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | manner. CSPs should:<br><br>a. implement and maintain a formal change management process to control changes to its production information processing facilities and systems; b. implement and maintain backup procedures for changes;<br><br>c. implement and maintain back-out or rollback procedures;<br><br>d. separate development, test, and production environments to reduce the risks of unauthorized access or changes to the operational system; and e. implement a patch management process. | ensures that all changes undergo appropriate approval and testing prior to implementation. The Tencent Cloud Change Release System enforces that only authorized personnel can execute change operations, and it retains comprehensive change-related logs, which are subject to regular audits.<br><br>Following the release of changes, Tencent Cloud verifies and monitors the changes in the production environment and records the outcomes. Additionally, Tencent Cloud has implemented stringent internal network segregation policies to ensure physical and logical separation between development, and production environments. Internal operations personnel are permitted to perform change operations only after obtaining the necessary approvals and authorizations, thereby preventing unauthorized data access and system modifications.<br><br>**In terms of patch management,** Tencent Cloud proactively identifies the latest patches and conducts thorough security testing before deployment to ensure patch safety. Internal business teams are regularly notified to perform patch upgrades and installations. Endpoint detection tools are employed to routinely scan for patch installation status, and automated alert tickets are generated for devices with overdue patch installations. |

## 5.4 Cloud Services Administration

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.16 | Cloud Service Administration | CSPs should implement cloud services administration controls to ensure the enforcement of policies, standards and procedures relating to the creation, maintenance and removal of privileged accounts used for managing cloud services and | **In terms of cloud-service privilege management,** Tencent Cloud has established access control management standards that define the requirements for managing privileged access and the associated authorization mechanisms. All user accounts are required to use unique identifiers, and employee accounts must comply with security baseline password policies, including requirements for password length, |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | supporting networks. CSPs should:<br><br>a. establish a formal registration and approval process in granting and modifying privileged rights to personnel administering the cloud services;<br><br>b. enforce password controls to administrative accounts based on the risk assessments and sensitivity of the system;<br><br>c. establish a formal access review and revocation process to review the adequacy of privileges and access levels, and de-provision or remove access in a timely manner;<br><br>d. implement a formal process to detect and terminate unauthorized access attempts in a timely manner. Access controls shall be established based on the risk assessments and sensitivity of the system and data;<br><br>e. put in place password security controls based on the risk assessments and sensitivity of the system and data;<br><br>f. establish procedures for password reset and first login for all accounts with access to the cloud service management network;<br><br>g. implement measures to ensure that the administration of cloud infrastructure is protected from unauthorized | complexity, account lockout, and reset procedures. For internal endpoints, operating systems, applications, and network devices, Tencent Cloud enforces login failure limits and session timeout policies.<br><br>A Zero Trust security management system is used to authenticate employee access. Access to internal resources requires completion of multi-factor authentication (MFA). Tencent Cloud continuously monitors employee account login activities in real time. If any anomalous login behaviour is detected, the system immediately contacts the account owner for verification and response, while logging the incident in detail.<br><br>Tencent Cloud has also implemented an authorization policy and a role-based access control (RBAC) matrix, maintaining mappings between personnel identities, job roles, and access levels across business systems. Regular internal access reviews are conducted to ensure that privileges are not misused or abused. Access rights that are no longer required are promptly revoked through appropriate follow-up actions.<br><br>In the production environment, Tencent Cloud has fully deployed bastion hosts to centrally manage administrator privileges for backend system components. Access to bastion hosts requires prior authorization and is restricted to designated internal operations personnel. Login to the bastion host is protected by MFA. All administrative operations are logged and stored centrally on a logging platform, which is regularly audited by Tencent Cloud's internal audit team. The logging platform includes rules for detecting abnormal user activities, and any identified anomalies are automatically escalated to the security team for investigation.<br><br>Through the **Cloud Access Management (CAM)** console, Tencent Cloud provides customers with secure permission assignment and sub-user management capabilities. CAM |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | changes;<br><br>h. implement procedures to log, via native systems or application logs, all administrators' activities;<br><br>i. establish controls to manage sessions based on the risk assessments and sensitivity of the system and data;<br><br>j. segregate duties and areas of responsibilities to reduce opportunities for unauthorized or unintentional modification or misuse of the information assets;<br><br>k. implement appropriate encryption and security protocols for transmitting credentials for non-console administrative access based on the risk assessments and sensitivity of the system and data;<br><br>l. implement controls (such as restrict privileged access to vendors on a need-to-have basis) for third party administrative access;<br><br>m. implement controls (such as changing service password at least twice annually) for all creation of service and application accounts; and<br><br>n. (additional measure) include more than one approver5 for system configuration changes, especially for changes that are significant or sensitive. | enables customers to define which actions and resources each user or role can access. Customers can also enable MFA for both primary and sub-accounts to enhance account security. CloudAudit provides comprehensive logging and continuous monitoring of user activities and API usage across Tencent Cloud infrastructure.<br><br>**In terms of configuration-change management,** Tencent Cloud has established standardized procedures for configuration change management, including defined processes for change assessment and approval. Critical or sensitive changes must undergo a comprehensive evaluation by relevant teams, including business, security, and quality assurance. Execution of such changes requires joint approval from both the R&D and business owners. |

## 5.5 Cloud Service Customer Access

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.17 | Cloud Service Customer Access | CSPs should implement cloud user access controls to ensure that policies, standards and procedures are established and implemented to govern the creation, maintenance and removal of user accounts to restrict access and safeguard user credentials to prevent unauthorized access to information and information systems. CSPs should:<br><br>a. establish a formal user registration process to grant, modify and restrict user access to the cloud services;<br><br>b. enforce control measures to user access to the cloud environment;<br><br>c. implement a formal process to allocate user passwords and require users to follow secure practices in the selection of passwords;<br><br>d. implement a formal process to ensure unauthorized access attempts are detected and terminated in a timely manner;<br><br>e. establish procedure for user password reset and first logon change;<br><br>f. implement password protection measures for all user login credentials;<br><br>g. implement user session management measure;<br><br>h. implement measures to monitor change in cloud user's | **In terms of cloud-user access-control management,** Tencent Cloud has established access control procedures that define standards for cloud customer account registration, management, and support. Customers are provided with access control features that enable them to define and enforce their own access policies for managing the cloud services they have purchased.<br><br>During the account registration process, customers are required to read and accept the Tencent Cloud Service Agreement via the official website, which outlines responsibilities and obligations related to access management. The management console serves as the central platform for customers to manage and control their cloud resources. Each customer is assigned a unique account identifier upon registration, and password policies are enforced. The console automatically verifies the uniqueness of account names. When logging into the console, identity credentials and operational commands are transmitted securely via HTTPS. Customers can also manage cloud services and data centrally through open APIs, which require authentication using access keys assigned to each customer. Tencent Cloud supports multi-factor authentication (MFA) to enhance the security of account logins and sensitive operations such as password changes. Password reset and modification functions are also available.<br><br>Tencent Cloud provides a **Cloud Access Management (CAM)** service to help customers securely and granularly manage access to Tencent Cloud products and resources. The primary account has full access to all associated resources and can create sub-accounts, assign identity credentials, and define permissions. Customers can configure password policies and session timeout settings for sub-accounts via the CAM console. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to encrypt passwords, avoiding plaintext storage. CAM also supports various MFA |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | administrator details;<br><br>i. implement measures for the self-service portal that is used for the creation and management of user account;<br><br>j. provide mechanisms for communication with cloud users; and<br><br>k. (additional measure) ensure strong encryption solutions are in place for software authentication tokens which grant users authorized access to cloud services. | methods and integrates with CloudAudit to track and review user activity logs.<br><br>**In terms of communication with cloud users,** Tencent Cloud has established multiple communication channels to facilitate interaction with external customers, including the official website console, email, and dedicated hotlines. The console provides a ticketing system that allows customers to report issues related to security, availability, and confidentiality. Tickets are prioritized through a tiered response mechanism. If frontline technical support cannot resolve an issue, the system automatically escalates the case to product or technical teams to ensure timely and effective resolution.<br><br>Tencent Cloud offers online and telephone support channels through its official website, enabling customers to report service-related issues. With geographically redundant customer service centers, Tencent Cloud provides 24/7 support to handle inquiries and deliver high-quality, around-the-clock technical assistance.<br><br>Customers may also select from various service plans that include access to dedicated support groups, technical account managers, and value-added services for enhanced support. |

## 5.6 Tenancy and Customer Isolation

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.18 | Tenancy and Customer Isolation | CSPs should implement tenancy and customer isolation controls to restrict user access within the same physical resource and segregate network and system environments such that the customers do not pose a risk to one another in terms of data loss, misuse and privacy violation. CSPs should:<br><br>a. implement control measures | **In terms of network-security architecture and management,** Tencent Cloud has established a comprehensive set of network security management standards and a defense-in-depth architecture. Through formal policies and procedures, Tencent Cloud defines network security controls, protection standards, and the roles and responsibilities of relevant personnel to ensure the secure operation of services hosted on its network.<br><br>Drawing on industry's best practices, Tencent Cloud designs its network security architecture based on |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | to protect each customers' hosted environment and sensitive data;<br><br>b. implement measures to limit sharing of resources between the cloud service delivery network, cloud service management network and CSP's internal network;<br><br>c. design, implement and manage secure network architecture to protect the cloud infrastructure, including (i) segregating networks by dividing them into separate network domains and separating them from the public network (i.e., Internet), ii) implementing appropriate access controls between network domains based on business needs and security requirements and iii) implementing appropriate network security controls to permit legitimate traffic and block unauthorized traffic. A test plan shall be formulated to verify and assess the implemented measures, develop compensating controls and ensure the network (both physical and virtual) is protected from unauthorized connections that may breach the access control policy;<br><br>d. implement control measures to manage information risks from the deployment of the cloud using virtualization technology;<br><br>e. limit access to data stored on | business functions and associated risk levels. Security zones are defined and segmented accordingly, with physical or logical isolation enforced between zones. Access control and perimeter defense mechanisms are implemented to safeguard the office, and production networks. Multiple layers of protection—including firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS mitigation, and web application firewalls—are deployed to defend against external threats from the internet.<br><br>Tencent Cloud also operates internal network monitoring systems to oversee routers, firewalls, and network servers, with alerting mechanisms in place for anomalies. Endpoint Detection and Response (EDR) tools are deployed across all server endpoints to enable comprehensive asset monitoring and control.<br><br>**In terms of tenant isolation,** in line with the principle of "data confidentiality," Tencent Cloud enforces strict tenant isolation through multiple security mechanisms. These include resource access control policies at the virtualization control layer, internal private network segmentation strategies, web console access control and identity authentication, session ID and access key management, and more. These measures ensure that each customer can only access their own purchased cloud resources, preventing unauthorized access, data leakage, or tampering between tenants.<br><br>Tencent Cloud also offers services such as **Virtual Private Cloud (VPC)**, **Cloud Firewall (CFW)**, and **Edge Security Acceleration Platform (EO)** to help customers implement secure network segmentation and perimeter protection.<br><br>**To enhance security in virtualized environments**, Tencent Cloud has developed internal virtualization security management standards. These define responsibilities for managing virtual machine (VM) resources, access control, and configuration management. A multi-layered virtualization security |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | a SAN; and<br>f. ensure access to data from customers is segregated from one another to prevent data co-mingling. | defense system is built using VM isolation and resource control, patch management and vulnerability mitigation, and hardening of the hypervisor layer. |

## 5.7 Cloud Resilience

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| 2.19 | Physical and environmental security | CSPs should implement physical and environmental security controls to prevent unauthorized physical access, damage or interference to the cloud environment and infrastructure with the use of appropriate procedures and assessments. CSPs should:<br>a. implement asset management controls;<br>b. implement control measures for offsite movement;<br>c. establish procedures (such as surveillance systems to monitor access, manning of physical security perimeter) for physical security and safety of the cloud information processing facilities;<br>d. implement procedures to restrict visitor access to the cloud information processing facilities;<br>e. establish guidelines for environmental threats and equipment power failures to all personnel working in the cloud information processing facilities; and | **In terms of physical-environment security,** Tencent Cloud has established a physical security management framework to regulate operational safety, promptly identify risks, and strengthen physical security controls.<br>All Tencent Cloud data centers—whether constructed or leased—are selected and operated in accordance with relevant international standards and local security requirements. In Singapore, Tencent Cloud operates four leased data centers. To ensure resilience and security, Tencent Cloud has implemented a comprehensive management system covering vendor onboarding, contractual obligations, and ongoing oversight. Annual internal and external audits are conducted, including on-site inspections of carrier-operated data centers, to verify compliance with Tencent Cloud's information security requirements.<br>Tencent Cloud requires data center operators to install smoke detectors, lightning protection and grounding systems, fire alarms and sprinkler systems, power supply and distribution systems, fresh air and air conditioning systems, and temperature monitoring devices. Operators must also provide 24/7 personnel support to ensure rapid resolution of equipment failures. Physical security emergency response plans must be established and regularly tested through drills involving data center staff.<br>**In terms of physical-access control,** Tencent Cloud mandates that data center operators |

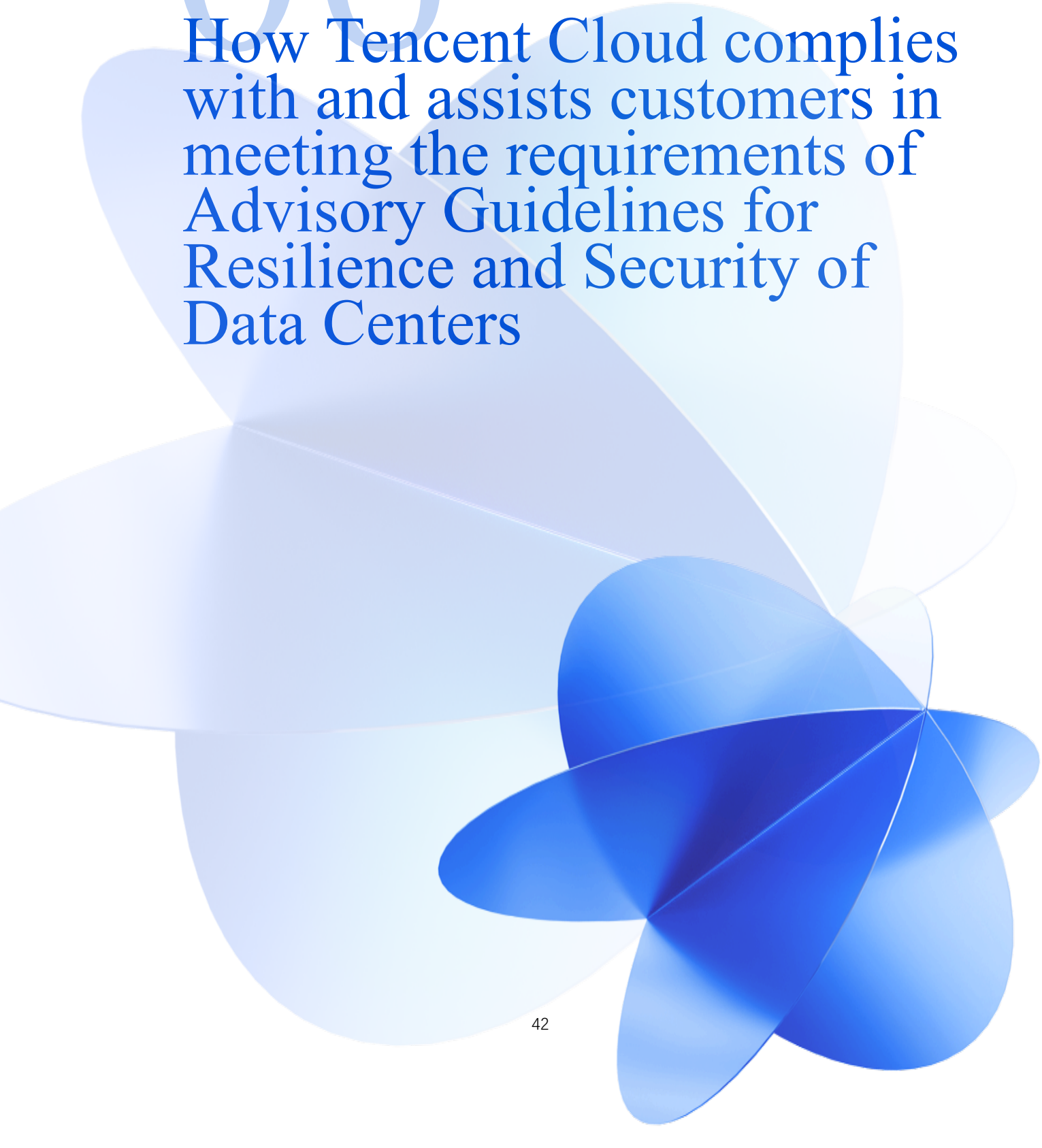
| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | f. perform review of the physical security controls to identify security and operational weaknesses in the DC. | implement formal access procedures, including identity verification and item registration for all personnel entering the facility. Regular reviews of access permissions are required to ensure appropriate access is maintained and unnecessary privileges are revoked in a timely manner. For external visitors, operators must enforce a visitor application and approval process. Only approved visitors may access designated areas during scheduled times and must be accompanied by authorized personnel. Equipment entering or leaving the data center (e.g., for installation, decommissioning, or relocation) must follow defined approval and inspection procedures.<br><br>**In terms of security guarding and surveillance,** Tencent Cloud requires the data-center operator's security personnel to conduct daily patrols of each computer room and equipment in strict accordance with the patrol checklist and schedule, sign off at every checkpoint and record the inspection time, and immediately initiate the data-center emergency-incident response process whenever infrastructure faults or security events are detected. Tencent Cloud also mandates that the operator maintain a 7×24 non-blind-spot video-surveillance and alarm system, staffed by a round-the-clock security control room, and ensure that surveillance records are securely retained for an adequate period.<br><br>**In terms of information-asset management,** Tencent Cloud has implemented an information asset management policy and lifecycle management process to classify, manage, and protect assets such as electronic data, hardware and virtual devices, infrastructure, application systems, and software. An asset management system is used to track hardware and software components, covering asset registration and binding, inventory checks and updates, and asset retirement or replacement. These measures ensure the stable operation of Tencent Cloud's underlying infrastructure and provide reliable |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | support for business systems. |
| 2.20 | Business continuity and disaster recovery | CSPs should implement business continuity and DR controls to ensure timely resumption from, and the possible prevention of interruptions to business activities and processes caused by failures of information systems and disasters. CSPs should:<br><br>a. develop, maintain and communicate a business continuity framework for the required cloud services;<br><br>b. develop and implement business continuity and DR plans;<br><br>c. establish a process to test and validate business continuity and DR plans to ensure adequacy and effectiveness of recovery requirements, and personnel's ability to execute emergency and recovery procedures;<br><br>d. (additional measure) conduct failover tests on cloud environment (minimally a representative environment with the same configurations) for:<br><br>i. all AZs within the Singapore region and any other failover services that CSP offers to customers; and<br><br>ii. global services necessary for the CSP's provision of cloud services to customers in Singapore. | Tencent Cloud operates data centers across multiple global regions, structured into geographic regions and availability zones, covering Mainland China, the Asia-Pacific region, North America, and Europe. Customers can flexibly deploy their data and systems across different regions or availability zones based on business growth and data security requirements, ensuring high availability and disaster recovery capabilities. Tencent Cloud mandates that cloud products within a single region adopt a multi–data center redundancy mechanism to ensure service continuity.<br><br>**In terms of internal business-continuity management,** Tencent Cloud has designed and implemented a business continuity management (BCM) framework tailored to its cloud computing environment. This comprehensive BCM system includes formal policies and standardized procedures covering business impact analysis (BIA), business continuity planning (BCP), emergency response and disaster recovery (DR), testing and exercises, and crisis management. Tencent Cloud's BCM system is certified to the ISO/IEC 22301 international standard for business continuity management.<br><br>To ensure the continuous availability of customer services, Tencent Cloud conducts business impact analyses for its cloud services and products to define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Based on these analyses, Tencent Cloud develops tailored response strategies and continuity plans, including detailed disaster recovery procedures for cloud products and critical business processes.<br><br>**Regarding business-continuity exercises and tests,** Tencent Cloud regularly conducts business continuity drills and tests in accordance with the BCP to validate the effectiveness and feasibility |

| No. | Domain | Summary of Controls | Tencent Cloud's Response |
|---|---|---|---|
| | | | of the plans and procedures. Each exercise is based on a predefined scenario, with associated risk assessments and mitigation measures to minimize potential service disruptions during testing. Disaster recovery drills often simulate realistic scenarios such as cyberattacks or large-scale system failures to comprehensively assess the resilience, responsiveness, and recovery capabilities of Tencent Cloud systems.<br><br>Following each exercise, relevant departments are required to compile a post-exercise report, document findings, implement corrective actions, and archive the report for future reference. |

06

# How Tencent Cloud complies with and assists customers in meeting the requirements of Advisory Guidelines for Resilience and Security of Data Centers



Advisory Guidelines for Resilience and Security of Data Centres provide best practice recommendations for enhancing the resilience and security of Singapore's computing infrastructure. These guidelines cover how Data Centre Operators (DCOs) can manage resilience and security risks through business continuity planning and appropriate mitigation measures. The provisions mainly focus on key risks to data centre resilience and security, risk management practices, additional measures for managing network risks, and the designation of responsible personnel.

In this section, Tencent Cloud summarizes the control requirements in the guidelines that are relevant to cloud service providers and explains how Tencent Cloud, as a cloud service provider, ensures its data centre management complies with these requirements.

## 6.1 Key Risks to Data Centre Resilience and Security

Section 2 of the guidelines identifies three core areas of risk for data center resilience and security: data center infrastructure, governance mechanisms, and cybersecurity. The causes and impact dimensions of these risks are as follows:

- Infrastructure Risks: These primarily stem from inadequate risk considerations during the design phase, including stability of power supply design, environmental controls (temperature and humidity), cable layout security, physical facility and tenant space protection, and compliance of site selection and design adaptability. Design flaws in these areas can directly affect the data center's ability to maintain continuous operations.
- Governance Risks: These arise from incomplete oversight mechanisms for operational risks, such as insufficient standardization of operational processes, inadequate incident response and management frameworks, and lack of risk controls during system and facility changes. These gaps can lead to unaddressed vulnerabilities during operations.
- Cybersecurity Risks: These mainly involve network attacks targeting data center operating systems and control systems, which may breach security boundaries and directly impact core business systems and data security.

Currently, Tencent Cloud operates four leased data centers in Singapore. To ensure resilience and security, Tencent Cloud has established a comprehensive management framework covering supplier onboarding, contractual obligations, and ongoing supervision:

- Supplier Selection: Tencent Cloud enforces strict security assessment and admission standards, conducting thorough due diligence on physical security (e.g., access control, surveillance, fire protection), information security management (e.g., encryption, access control), and business continuity capabilities (e.g., disaster recovery plans, fault recovery mechanisms) to ensure compliance with high security standards.
- Contractual Agreements: Tencent Cloud formalizes responsibilities and service boundaries through standardized contracts, clearly defining service scope and quantifying key service standards such as availability levels, thereby ensuring contractual assurance of service quality.
- Operational Oversight: Tencent Cloud implements continuous monitoring and evaluation mechanisms, regularly assessing the technical capabilities, service responsiveness, and risk management effectiveness of data center operators. Tencent Cloud requires

operators to submit SLA compliance reports periodically, covering major incident handling, key performance indicators, and maintenance summaries. Performance evaluations are conducted regularly and serve as a critical reference for future supplier engagements.

## 6.2 Managing Data Centre Resilience and Security Risks

Section 3 of the guidelines recommends that DCOs effectively manage risks across infrastructure, governance, and cybersecurity domains. DCOs should establish a Business Continuity Management (BCM) framework to mitigate the risk of service disruptions during unexpected events, ensuring uninterrupted delivery of critical services and minimizing business impact.

Tencent Cloud includes BCM capabilities as a core criterion in supplier onboarding and performance evaluations, ensuring compliance and effectiveness through multi-dimensional controls. Tencent Cloud conducts annual internal and external audits, including on-site inspections, to verify whether operators have established a robust BCM framework—covering identification of critical services, business impact analysis, risk assessments, continuity and disaster recovery plans, and professional operations teams. Tencent Cloud also evaluates whether operators conduct regular staff training and scheduled continuity drills, and whether they optimize BCM plans based on drill outcomes.

Furthermore, Tencent Cloud requires operators to align their risk and continuity management systems with international standards such as ISO 22301 (Business Continuity Management), ISO 27001 (Information Security Management), ISO 31000 (Risk Management), ISO 22237 (Data Centre Infrastructure), and TIA-942 (Telecommunications Infrastructure for Data Centres).

## 6.3 Managing Network Risks and Additional Measures

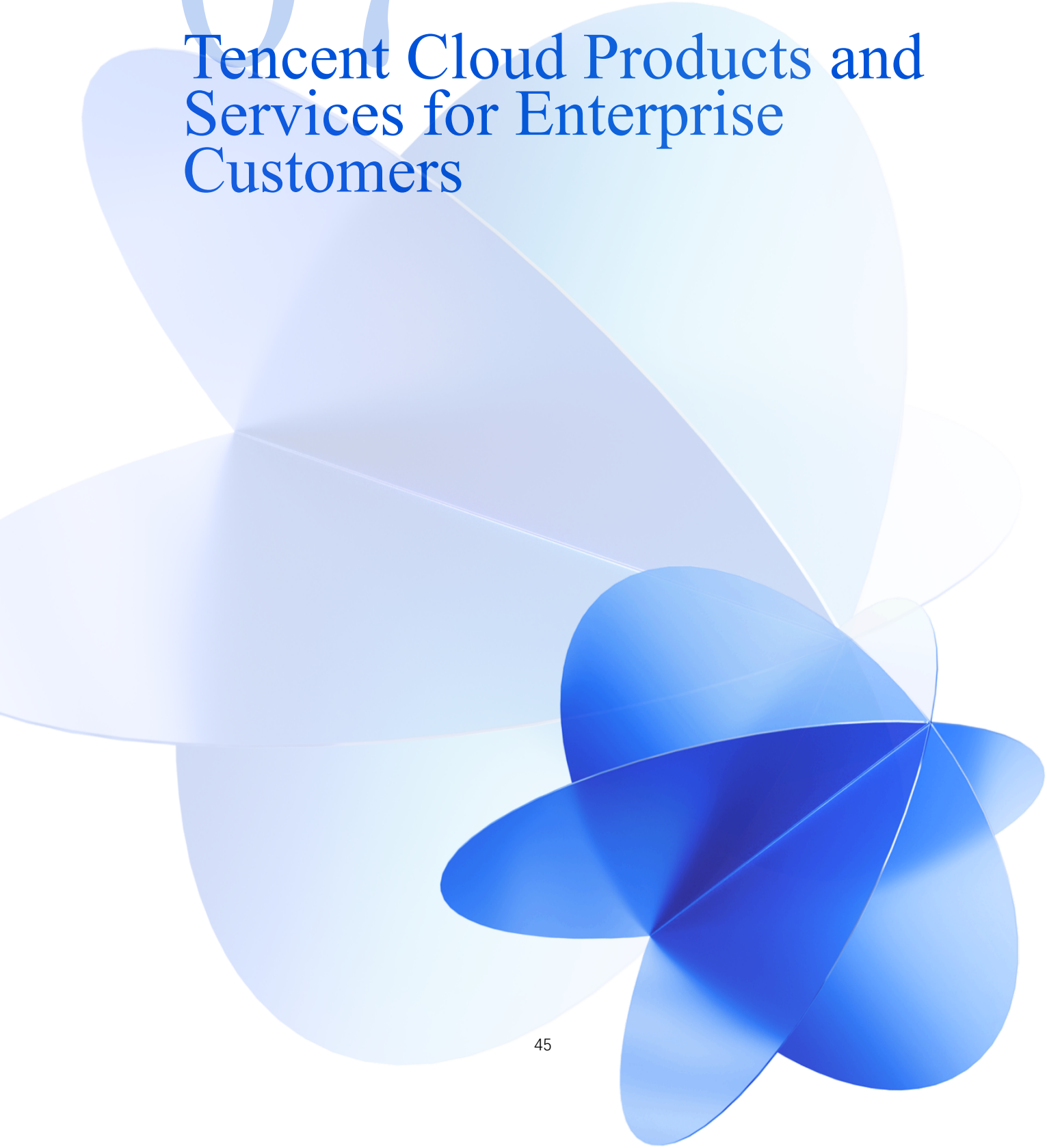
Section 4 of the guidelines specifies that DCOs should tailor network threat management measures to the operational needs of each data centre and ensure adequate cybersecurity controls for networks and systems.

Tencent Cloud has established a robust supply chain security management framework, including stringent supplier security assessments, regular reviews, and clearly defined outsourcing agreements. Tencent Cloud focuses on evaluating operators' cybersecurity controls across areas such as information security management systems, HR security, third-party management, regulatory compliance, audit logging and monitoring, system configuration, security testing, procurement and development security, data encryption, access control, and network isolation. These measures form a comprehensive cybersecurity protection system, ensuring that suppliers do not compromise Tencent Cloud's ability to deliver services and that customer data confidentiality and integrity are maintained.

For details on how Tencent Cloud manages its own service resilience and security risks, please refer to Section 5: **How Tencent Cloud complies with and assists customers in meeting the requirements of Advisory Guidelines for Resilience and Security of Cloud Services**."

07

# Tencent Cloud Products and Services for Enterprise Customers



Tencent Cloud leverages cloud and AI technologies to deliver a comprehensive suite of full-stack products, meeting diverse enterprise needs across infrastructure, platform solutions, and application layers. These offerings empower businesses to accelerate digital transformation, enhance operational resilience, and strengthen security posture. Backed by robust, reliable, and efficient services, Tencent Cloud helps enterprises achieve growth and competitiveness while addressing both foundational and business security requirements. The following sections provide an overview of selected Tencent Cloud **products and services**. For more details, please visit the Tencent Cloud official website for a complete list of products and solutions.

## 7.1 Security Products

- **Web Application Firewall (WAF)**

**Web Application Firewall (WAF)** is an AI-powered, one-stop solution for mitigating web application operational risks. It works by redirecting traffic originally destined for web business sites to Tencent Cloud's WAF protection cluster nodes, where threats are filtered and cleaned before safe traffic is returned to the business site. This ensures that all traffic reaching the customer's site is secure and trustworthy. Tencent Cloud WAF effectively defends against OWASP attacks such as SQL injection, XSS cross-site scripting, Trojan uploads, and unauthorized access. It also filters CC attacks, provides 0-day vulnerability patches, prevents webpage tampering, and offers comprehensive protection for both system and business security.

- **Cloud Firewall (CFW)**

**Cloud Firewall (CFW)** is a SaaS-based firewall designed for public cloud environments. It provides internet boundary protection and addresses unified management of cloud access control and log auditing. In addition to traditional firewall capabilities, CFW supports multi-tenancy and elastic scalability, serving as a foundational network security infrastructure for businesses migrating to the cloud.

- **Anti-DDoS Protection**

**Anti-DDoS** offers comprehensive, efficient, and professional protection against DDoS attacks. It provides multiple solutions such as high-defence packages and high-defence IPs. Leveraging abundant, high-quality resources and continuously evolving proprietary and AI-driven detection algorithms cleansing algorithms, Anti-DDoS ensures stable and secure business operations.

- **EO Edge Security Acceleration Platform (EO)**

**Edge Security Acceleration Platform (EO)** leverages Tencent's global edge nodes to deliver security protection and acceleration services for overseas markets. It offers DDoS protection, intelligent web defence, bot/crawler attack mitigation, DNS resolution, and customizable access control based on business needs, safeguarding enterprises across industries and enhancing user experience.

- **Container Security Service (TCSS)**

**Tencent Cloud Container Security Service (TCSS)** provides container asset management, image security, and runtime intrusion detection, ensuring security throughout the container lifecycle—from image creation and storage to runtime—helping enterprises build a robust container security framework.

- **Vulnerability Scanning Service (VSS)**

Vulnerability Scanning Service (VSS) automatically detects enterprise network assets and identifies risks. Backed by Tencent's decades of security expertise, VSS performs regular security scans, continuous risk alerts, and vulnerability detection for network devices and application services, offering professional remediation advice to reduce security risks.

- **Penetration Testing Service (PTS)**

Cloud Pressure Testing (PTS) delivers security penetration testing for web applications and mobile apps, covering the entire vulnerability lifecycle—from discovery and exploitation to remediation and validation. By simulating hacker techniques and vulnerability discovery methods, PTS identifies the weakest points in target systems. Tests are conducted under customer authorization using controlled, non-destructive methods, providing hardening recommendations to enhance system security. Tencent Cloud's PTS is performed by Tencent Security Lab experts and offers black-box, white-box, and gray-box testing for comprehensive risk identification.

- **Cloud Workload Protection Platform (CWPP)**

**Cloud Workload Protection Platform (CWPP),** is a multi-cloud host security solution that leverages Tencent's extensive threat intelligence and machine learning to provide asset management, malware detection, intrusion prevention, vulnerability alerts, and baseline compliance, helping enterprises build a secure server environment.

- **Cloud Security Center (CSC)**

**Cloud Security Center (CSC)** is Tencent Cloud's unified security management platform, integrating asset, risk, and alert centers with advanced security management to enable a closed-loop security operation covering threat detection, incident response, and forensic analysis.

- Asset Center: Automatically synchronizes 34 types of Tencent Cloud assets and supports manual addition of non-Tencent IPs and domains for unified management.
- Risk Center: Detects six major risks—port, vulnerability, weak password, content, cloud resource configuration, and service exposure—and categorizes them for management.
- Alert Center: Aggregates logs from Cloud Firewall, WAF, and CWPP, analyzes and consolidates alerts for unified display and handling.
- Advanced Security Management: Supports centralized account management and simulated attack defense validation.

- **Key Management Service (KMS)**

**Key Management Service (KMS)** enables secure key creation and management, ensuring confidentiality, integrity, and availability. It meets regulatory and compliance requirements

using FIPS 140-2 certified HSMs for key generation and protection, secure transmission protocols, and multi-data center deployment with hot and cold backups for high availability. KMS integrates seamlessly with services like object storage, distributed databases, and cloud disks for encryption.

- **Data Security Governance Center (DSGC)**

Tencent Cloud Data Security Governance Center (DSGC) is a data security operations platform that combines sensitive data discovery, classification, data mapping, and anomaly detection. It helps enterprises automatically inventory data assets, classify and assess risks, and collaborate with Tencent Cloud's security capabilities to form a closed-loop data protection network, maximizing security effectiveness.

## 7.2 Cloud Computing and Networking Products

- **Cloud Virtual Machine (CVM)**

Cloud Virtual Machine (CVM) is a high-speed, stable cloud virtual host and one of Tencent Cloud's core products, providing scalable computing capacity in the cloud. Key features include:

- Efficiency – Rapid Deployment: Some CVM instances can be created in as little as 10 seconds, with single-region support for thousands of instances per minute.
- Ease of Use – Cross-Zone Hot Migration: Enables hot migration across availability zones within the same region without service interruption.
- Reliability – Robust Disaster Recovery: Tencent Cloud's unique placement groups offer multi-level disaster recovery across physical machines, racks, and switches within availability zones, ensuring comprehensive resilience.

- **Cloud Bare Metal (CBM)**

Cloud Bare Metal (CBM) is a scalable and high-performance cloud-based bare metal instance featuring the lossless performance and resource security isolation of physical machines. It slashes the time to get physical machines for minutes. Make your cloud resources easy to use and secure as CBM instances run in public cloud VPCs, which enables smooth communication among Tencent Cloud products.

- **Auto Scaling (AS)**

Auto Scaling (AS) enables efficient management of computing resources. Customers can configure scheduled or real-time policies to adjust CVM instance counts and deploy environments automatically, ensuring smooth business operations. During peak demand, AS scales up instances to maintain performance; during low demand, it scales down to reduce costs. AS helps stabilize workloads, mitigate sudden traffic spikes or CC attacks, and supports minute-level scaling for fluctuating usage patterns.

- **Tencent Kubernetes Engine (TKE)**

Tencent Kubernetes Engine (TKE) provides high-performance container management based on native Kubernetes, fully compatible with Kubernetes APIs and extended with Tencent Cloud plugins for Cloud Block Storage (CBS), Cloud Load Balancer (CLB), and more. TKE offers efficient deployment, resource scheduling, service discovery, and dynamic scaling, ensuring environment consistency across development, testing, and operations.

- **Tencent Container Registry (TCR)**

Tencent Cloud Container Registry (TCR) delivers secure, high-performance container image hosting and distribution. Customers can create dedicated instances across multiple global regions for faster image pulls and reduced bandwidth costs. TCR supports fine-grained access control, P2P acceleration for large-scale deployments, and flexible integration with CI/CD workflows for rapid DevOps implementation.

- **Virtual Private Cloud (VPC)**

Virtual Private Cloud (VPC) provides an isolated cloud network environment for Tencent Cloud resources, enabling software-defined networking for IP addresses, subnets, routing tables, ACLs, and flow logs. VPC supports multiple internet connectivity options such as Elastic IP and NAT gateways, as well as VPN Connection or Direct Connect (DC)for hybrid cloud architectures.

- **VPN Connection**

VPN Connection uses tunneling technology to securely link on-premises data centers with Tencent Cloud resources over the Internet. It offers simple configuration, real-time cloud-side activation, high reliability, and gateway redundancy, ensuring stable business connectivity and enabling disaster recovery and hybrid cloud deployments.

## 7.3 Storage and Database Products

- **CLS Cloud Log Service (CLS)**

Cloud Log Service (CLS) is a one-stop log service platform offering log collection, storage, retrieval, real-time consumption, and delivery. Built on a highly available distributed architecture with multi-redundant backups, CLS ensures data reliability and service continuity for operational monitoring, security auditing, and analytics.

- **Cloud Object Storage (COS)**

Cloud Object Storage (COS) is a distributed storage service supporting massive data volumes without directory or format restrictions, accessible via HTTP/HTTPS. COS provides multi-architecture redundancy, cross-region disaster recovery, and anti-hotlinking features for secure and durable data storage.

- **Cloud Block Storage (CBS)**

Cloud Block Storage (CBS) offers persistent block-level storage for CVM instances, with multi-replica redundancy within availability zones to prevent single-point failures. CBS supports multiple disk types, low-latency performance, and elastic capacity adjustments within minutes.

- **Cloud File Storage (CFS)**

Cloud File Storage (CFS) provides secure, scalable shared file storage for cloud servers, container services, and batch computing. With triple redundancy and isolation controls, CFS ensures high availability and reliability for enterprise workloads.

- **Cloud Native Database TDSQL-C**

Cloud Native Database TDSQL-C is Tencent Cloud's next-generation cloud-native relational database, combining traditional database strengths with cloud computing and new hardware technologies. It supports MySQL and PostgreSQL compatibility, high elasticity, massive storage, and second-level failover for robust data protection.

- **TencentDB for MySQL**

TencentDB for MySQL enables easy deployment and use of MySQL databases in the cloud. Customers can deploy scalable MySQL instances within minutes. The service provides a complete set of database operation and maintenance solutions, including backup and restore, monitoring, rapid scaling, and data migration, simplifying IT operations and allowing customers to focus on business growth.

- **Tencent Cloud Distributed Cache (Redis ® OSS-Compatible)**

Tencent Cloud Distributed Cache (Redis ® OSS-Compatible) offers a cache and storage service compatible with the Redis protocol. Its rich data structures support diverse business scenarios. The service provides hot standby, automatic failover, data backup, fault migration, instance monitoring, online scaling, and data restoration, delivering a comprehensive database solution.

- **TencentDB for MongoDB**

TencentDB for MongoDB is a high-performance NoSQL database built on the globally popular MongoDB engine. It is fully compatible with the MongoDB protocol and offers robust monitoring, elastic scalability, and comprehensive backup and recovery mechanisms. Each instance cluster is backed up daily by default, with real-time dual hot standby and five-day cold backup downloads.

- **DTS Data Transmission Service (DTS)**

Data Transfer Service(DTS) supports migration for multiple relational and NoSQL databases, including MySQL, MariaDB, PostgreSQL, Redis, and MongoDB. It enables seamless database migration to the cloud without service interruption, builds high-availability disaster recovery architectures through real-time synchronization, and supports data subscription for analytics and asynchronous business decoupling.

## 7.4 Development and Operations Products

- **Cloud Access Management (CAM)**

Cloud Access Management (CAM) provides a secure and fine-grained user and permission management system for Tencent Cloud resources. Customers can create, manage, and delete users or roles, and control their actions and resource access through identity and policy

management. CAM also supports federated authentication for integration with enterprise identity systems, enabling seamless access for employees and services.

- **Cloud Audit**

CloudAudit offers compliance checks, operation auditing, and risk monitoring for Tencent Cloud accounts. It records logs, continuously monitors account activities across Tencent Cloud infrastructure, and retains historical records of operations performed via the console, APIs, CLI tools, and other services. These records simplify security analysis, resource tracking, and troubleshooting.

- **Bastion Host (BH)**

Bastion Host (BH) provides proxy access and intelligent operation auditing for IT assets. Acting as a unified entry point for internal asset management, BH eliminates the need to remember multiple addresses and credentials. It supports granular authorization based on user, asset, account, and operation permissions, ensuring least privilege access. BH analyzes multiple dimensions—time, commands, upload/download actions, IP addresses, servers, and usernames—to detect and alert abnormal behavior, preventing insider threats.

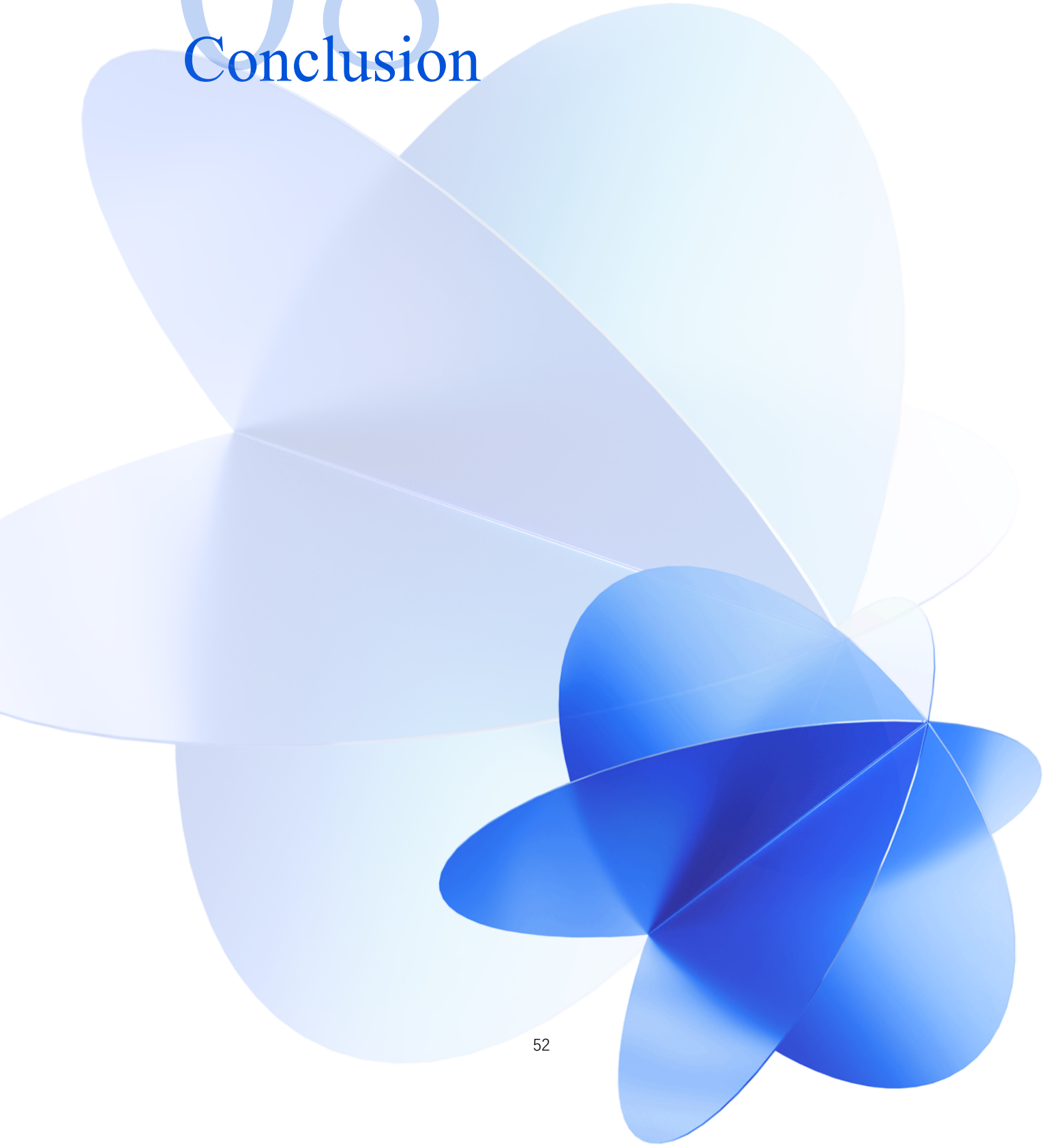
- **Tencent Cloud Observability Platform (TCOP)**

Tencent Cloud's Observability Platform (TCOP) collects and visualizes monitoring metrics for Tencent Cloud products and custom configurations, supporting alert settings for specific indicators. It offers multi-dimensional monitoring, intelligent data analysis, real-time anomaly alerts, and customizable reporting, enabling customers to maintain precise control over business and cloud product health.

- **Cloud Native Build (CNB)**

Cloud Native Build (CNB) provides code hosting, cloud-native build, development tools, AI-assisted coding, and artifact management. Based on the Docker ecosystem, CNB abstracts environments, caches, and plugins, and uses declarative syntax to help developers build software more efficiently.

# 08 Conclusion



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

This guide is based on key regulatory requirements issued by Singapore's Infocomm Media Development Authority (IMDA) and aims to provide customers with a comprehensive and transparent overview of how Tencent Cloud supports compliance for cloud-hosted systems and data. Our goal is to help enterprises confidently and securely migrate systems and data to the cloud. Through this guide, Tencent Cloud seeks to assist customers in meeting IMDA compliance standards effectively while enabling digital innovation and business growth.

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

# 09 Version History

| Date | Version | Detail |
| --- | --- | --- |
| April 2016 | V1.0 | Initial Release |
| | | |