Tencent Cloud

Tencent Cloud User Guide to Cyber Security Regulations & Guidelines in Indonesia

April 2026

CONTENTS

01 Overview

Against the backdrop of the global digital wave, information technology has been deeply integrated into Indonesia's international trade and economic growth processes, becoming a core engine driving industrial upgrading and unleashing economic vitality. In this context, the Indonesian government and the Ministry of Communication and Digital Affairs (hereinafter referred to as "Komdigi") have a profound understanding that building a sound legal infrastructure and regulatory system is a key guarantee for supporting the development of information technology. This initiative not only aims to regulate the application scenarios of information technology and prevent the risks of abuse, but also is committed to building a solid security barrier for the digital ecosystem through standardized supervision, laying a solid foundation for the sustainable development of the digital economy. Based on the above development vision and regulatory demands, the Indonesian government and the Ministry of Communication and Digital Affairs have formulated a series of specific and clear regulatory requirements for the field of electronic information systems and transactions. This series of regulatory measures not only demonstrates Indonesia's strategic determination to vigorously develop the digital economy and seize the opportunities of digital transformation, but also reflects its firm commitment to strengthening industry accountability mechanisms and ensuring cybersecurity and data security in the context of the rapid expansion of digital space, providing clear guidance for the standardized and secure development of Indonesia's digital ecosystem.

Tencent Cloud closely monitors the latest regulatory developments and official publications of the Government of Indonesia and the Ministry of Communication and Informatics, and is committed to supporting customers in Indonesia in meeting the regulatory requirements of the relevant authorities. This document explains how Tencent Cloud assists customers in complying with the key regulatory guidelines and notices of interest to customers below：

- Regulation No 11 Year 2008 – Electronic Information and Transaction
- Regulation No 19 Year 2016 – Electronic Information and Transaction
- Regulation No 71 Year 2019 – The Implementation of Electronic Systems and Transaction
- Regulation No 5 Year 2020 – Private Electronic System Providers
- Regulation No 10 Year 2021 – Amendment to Regulation No. 5 of 2020

02

Tencent Cloud Security and Privacy Compliance

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

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

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

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

2.1 Global Compliance

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

2.2 ISO/IEC Certification

ISO/IEC 22301: 2019 Certification	ISO/IEC 22301:2019 is an international standard for Business Continuity Management (BCM), providing a comprehensive and universal methodology to help organizations identify and respond to potential disruptive events, ensure the continuity of critical operations, reduce risks, and protect against significant impacts. Tencent Cloud has obtained ISO/IEC 22301:2019 certification, demonstrating that it has established formal business continuity management processes to ensure operational stability and resilience.

ISO/IEC 27001: 2022 Certification	ISO/IEC 27001:2022 Information Security Management System is recognized globally as one of the most authoritative, rigorous, and widely adopted certification standards in the field of information security. Achieving this certification signifies that an organization has established a scientific and effective information security management framework to align business strategy with security governance, ensuring that information security risks are properly controlled and addressed. Obtaining ISO/IEC 27001:2022 certification further demonstrates Tencent Cloud's commitment to security and confirms its capability to deliver secure and reliable cloud products and services.
ISO/IEC 20000-1: 2018 Certification	ISO/IEC 20000-1:2018 is an international standard for IT Service Management (ITSM). It defines a structured approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving IT service management systems. The standard helps organizations consistently identify and manage IT-related issues, strengthen communication with users, and build a standardized service framework that supports continuous improvement. Tencent Cloud has obtained ISO/IEC 20000-1:2018 certification, covering cloud computing services, hosting services, and disaster recovery services, demonstrating its commitment to delivering reliable and customer-focused IT service management.
ISO/IEC 9001: 2015 Certification	ISO 9001:2015 is a globally recognized and mature quality management system standard. It provides a comprehensive framework and guiding principles for managing the entire lifecycle of products and services, ensuring consistent and stable delivery quality. Tencent Cloud has obtained ISO 9001 certification, covering cloud computing services, hosting services, and disaster recovery services. By implementing a quality management system, Tencent Cloud effectively achieves its quality objectives and ensures the reliability and operational excellence of its cloud products and services.
ISO/IEC 27017: 2015 Certification	ISO/IEC 27017:2015 is an international standard that supplements ISO/IEC 27002:2013, providing practical guidelines for cloud service information security. It offers specific security controls and implementation guidance for both cloud service providers and customers, strengthening the management of threats and risks unique to cloud computing environments. Tencent Cloud has obtained ISO/IEC 27017:2015 certification, demonstrating its adherence to internationally recognized best practices and its commitment to building a comprehensive cloud security management system that enhances overall cloud security capabilities.
ISO/IEC 27018: 2014 Certification	ISO/IEC 27018:2014 is a globally recognized standard for the protection of personally identifiable information (PII) in public cloud environments. It provides a set of best practices for cloud service providers to safeguard user privacy and ensure the security of personal data in cloud computing. Tencent Cloud has obtained ISO/IEC 27018:2014 certification, signifying that its personal information management system complies with stringent international requirements for personal data protection, offering customers greater trust and assurance in cloud security.
ISO/IEC 29151: 2017 Certification	ISO/IEC 29151:2017 is an international standard that defines control objectives, controls, and implementation guidelines for processing personally identifiable information (PII) to address risks and privacy requirements identified through risk and impact assessments.

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

2.3 Regional and Industry Compliance

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

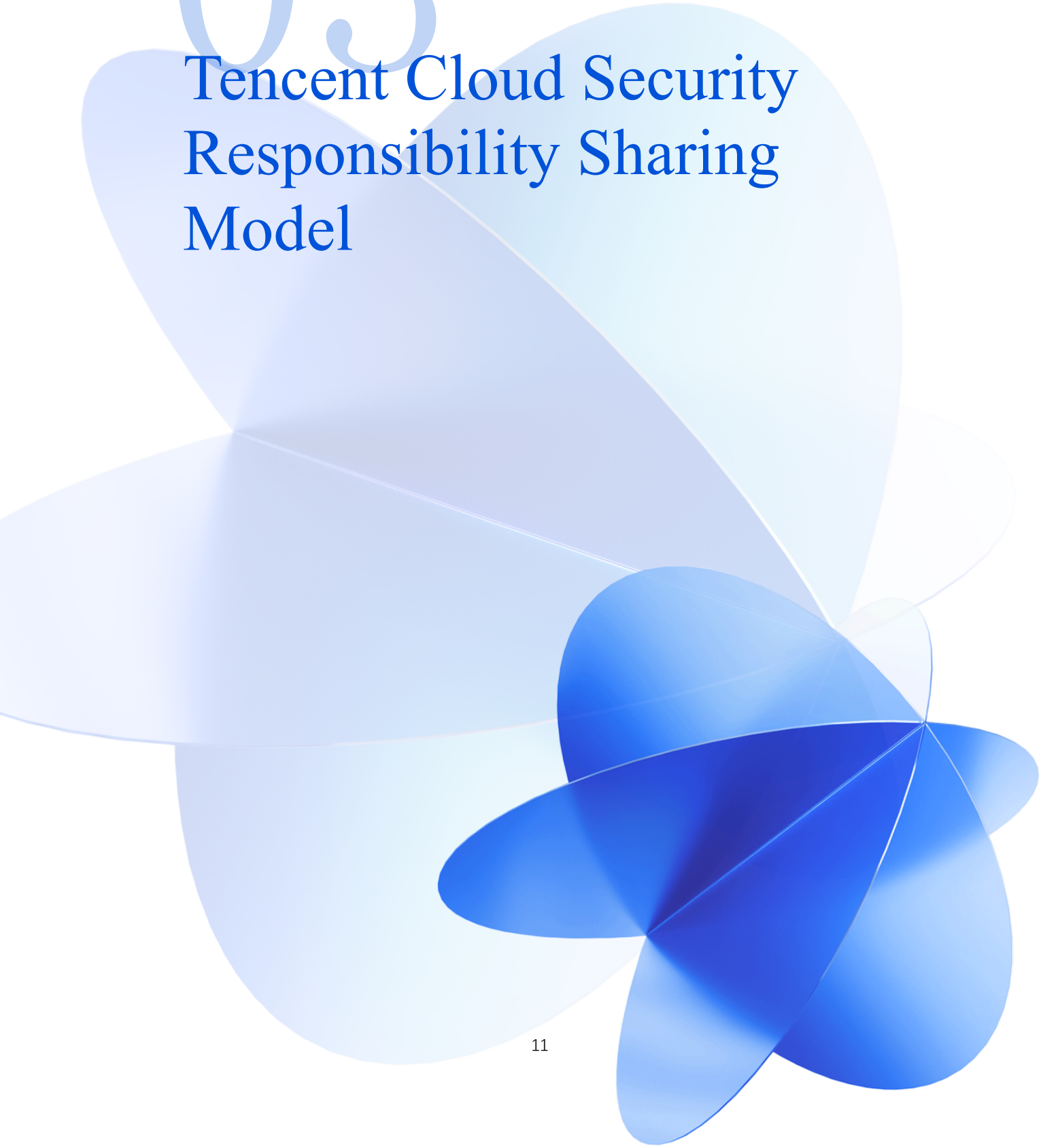
	meet the stringent requirements for financial services in Singapore and Southeast Asia.
Data Protection Trustmark (DPTM) [Singapore]	The Data Protection Trustmark (DPTM) was developed by Singapore's Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA) to help organizations demonstrate responsible data protection practices. Tencent Cloud has obtained the DPTM certification, indicating that it adopts robust and accountable data protection measures for customers, business partners, and regulators, and is capable of safeguarding the personal data it collects.
Cyber Trust Mark (CTM) [Singapore]	The Cyber Trust Mark (CTM) is a national-level cybersecurity certification launched by the Cyber Security Agency (CSA) of Singapore. The CTM framework adopts a risk-based methodology, covering 22 sub-domains across 4 core areas: governance and risk management, cybersecurity operations, resilience, supply chain and personnel security, as well as continuous improvement and leading practices. Tencent Cloud has attained the highest level (Tier 5) of the Cyber Trustmark (CTM). This certification underscores Tencent Cloud's advanced capabilities in cybersecurity governance, risk management, and operational resilience, positioning it as a trusted cloud service provider for regulated and high-demand sectors across the Asia-Pacific region.
KISMS [Korea]	The Korean Information Security Management System (K-ISMS) certification is a government-backed standard designed to help organizations in Korea consistently and securely protect their information assets in accordance with applicable laws and regulations. Tencent Cloud has obtained K-ISMS certification, enabling customers in Korea to demonstrate compliance with local legal requirements for safeguarding critical digital information assets. This achievement also reflects Tencent Cloud's enhanced capabilities in information security and threat response, ensuring more effective mitigation of potential security risks.
IT compliance audit in Malaysian financial industry	Bank Negara Malaysia (BNM), the Securities Commission (SC), and other Malaysian financial regulatory authorities have issued regulations for the financial services industry to govern the application of information technology in banking, insurance, securities, and other financial services in Malaysia, ensuring the reliability, security, and stability of financial information systems. Tencent Cloud demonstrates compliance through independent third-party audits, proving that the cloud services provided to financial customers in Malaysia strictly adhere to the regulatory requirements of the Malaysian financial industry.
IT compliance audit in Hong Kong Special Administrative Region (HKSAR) 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. 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. Independent third-party audits demonstrate Tencent Cloud's compliance with Thailand's stringent financial industry regulatory requirements and its commitment to providing high-quality, compliant cloud services to financial sector customers.
IT compliance audit in Indonesian financial industry	Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan, OJK), and other Indonesian financial regulatory authorities have issued regulations for the financial services industry. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits confirm that Tencent Cloud strictly complies with the regulatory requirements of Indonesia's financial industry when providing cloud services to financial customers.
Indonesia SNI 27001	SNI 27001 certification, a national standard for information security management systems (ISMS) regulated by Badan Standardisasi Nasional (BSN) and accredited by independent third-party auditors. The SNI 27001 framework adopts a risk-based approach, with core requirements covering key dimensions: Establishment and continuous operation of a formal ISMS, Comprehensive risk assessment and targeted control measures, Compliance with local information security regulations and 14 critical security domains and Regular internal audits, management reviews, and continuous improvement. Tencent Cloud has obtained Indonesia's SNI 27001 certification, Tencent Cloud has demonstrated excellence in protecting information asset confidentiality, integrity, and availability—extending to cloud-specific security scenarios. The certification reflects Tencent Cloud's mature security management system and its ability to address evolving cyber risks in the Indonesian market.
IT compliance audit in Philippines financial industry	Financial institutions in the Philippines are required to comply with regulations issued by the Bangko Sentral ng Pilipinas (BSP) and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's ability to comply with the stringent regulatory requirements of the Philippine financial industry and its commitment to providing high-quality, compliant cloud services to financial sector customers.
The Motion Picture Association of America (MPAA)	The Motion Picture Association of America (MPAA) has established a set of best practice standards for securely storing, processing, and transmitting protected media content. This implementation guidance is intended to help application and cloud service providers working with MPAA members understand the requirements for content security. The components of the MPAA Content Security Model reference relevant ISO standards (ISO 27001 and ISO 27002), recognized security standards (such as NIST, CSA, ISACA, and SANS), and industry best practices. Tencent Cloud has obtained certifications including ISO 27001, ISO 27017,

	ISO 27018, PCI DSS, and CSA STAR, and has conducted self-assessments to ensure that its content management processes comply with the MPAA Content Security Model.
HIPAA [US]	Health Insurance Portability and Accountability Act (HIPAA) is to promote the use of electronic health records to improve the efficiency and quality of the healthcare system through enhanced information sharing. HIPAA focuses on protecting the security (including availability, integrity, and confidentiality) and privacy of Protected Health Information (PHI) during creation, receipt, maintenance, and transmission by covered entities and their business associates. Entities subject to HIPAA are required to implement appropriate security measures when processing, maintaining, and storing PHI. Tencent Cloud conducts self-assessments to ensure its capability to protect personal information and the effectiveness of its control measures in compliance with HIPAA requirements.
SEC Rule 17a-4 [US]	Tencent Cloud Object Storage (COS) has been certified by an independent third-party assessment firm specializing in records management and information governance, based on the technical requirements of the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Commodity Futures Trading Commission (CFTC). This certification provides assurance for customers operating in highly regulated environments, such as the financial services industry, regarding the non-rewriteable, non-erasable preservation method and object lock feature of Tencent COS, demonstrating Tencent Cloud's commitment to delivering secure and industry-compliant cloud products.
The center for Financial Industry Information Systems (FISC) [Japan]	To enhance the security of financial institutions, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions provide effective guidance for Japanese banks and financial institutions in building secure information systems and ensuring their stable operation. Tencent Cloud has assessed its control measures against these guidelines to confirm that relevant measures meet the requirements of the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions.
BS10012: 2017 [UK]	BS10012:2017 was published by the British Standards Institution to provide organizations with a compliance framework and good practices for privacy protection. It guides businesses in establishing and maintaining a Personal Information Management System (PIMS) to ensure adequate and appropriate controls for protecting personal information. The standard has been updated and revised to align with the General Data Protection Regulation (GDPR). Tencent Cloud has obtained BS10012:2017 certification, demonstrating that its personal information management system meets international standards and industry best practices, enabling customers to better comply with GDPR privacy protection requirements.
CISPE Code of Conduct [EU]	The CISPE Code of Conduct is a pan-European, sector-specific code for cloud infrastructure service providers under Article 40 of the EU General Data Protection Regulation (GDPR). It helps organizations across Europe accelerate the development of GDPR compliant cloud-based services for consumers, businesses, and institutions. Tencent Cloud has awarded "Candidate" mark of CISPE Code of Conduct, which means the cloud service provider has fulfilled the self-assessment against the CISPE Code of Conduct requirements.

NIST CSF Certification	NIST CSF is a framework that focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risk as part of an organization's risk management process. It helps organizations adjust and prioritize their cybersecurity activities based on business needs, risk tolerance, and resources, and improve security and resilience by applying the framework's risk management principles and guidelines. Tencent Cloud has obtained NIST CSF certification from an independent third-party organization, which affirms the capability of its cybersecurity defense system and demonstrates its ability to effectively identify, resist, respond to, and manage security risks, protecting cloud assets and data and enhancing confidence in security and stability.
PCI DSS Certification	The Payment Card Industry Data Security Standard (PCI DSS) is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC). To enhance the security of cardholder data, PCI DSS provides a globally unified benchmark for technical and operational requirements to protect account data. It applies to all entities involved in payment card processing, such as merchants, processors, acquiring institutions, issuing institutions, service providers, and other entities that store, process, or transmit cardholder data. Tencent Cloud has passed PCI DSS certification and obtained Grade 1 Service Provider qualification, demonstrating its capability to provide secure and reliable payment services and protect cardholder data.
GxP Compliance	In the healthcare industry, GxP refers to a set of regulations, guidelines, or industry best practices that govern compliance-related activities for medical products such as pharmaceuticals, medical devices, and medical software applications. Tencent Cloud has published a GxP compliance white paper to explain how its management processes and technical measures help customers meet the requirements of GxP computerized systems and ensure the confidentiality, integrity, and availability of business data hosted on Tencent Cloud.

03 Tencent Cloud Security Responsibility Sharing Model



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

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

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

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

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

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

development, release, operation and maintenance, and ongoing monitoring.

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

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

04

Tencent Cloud Global Infrastructure

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

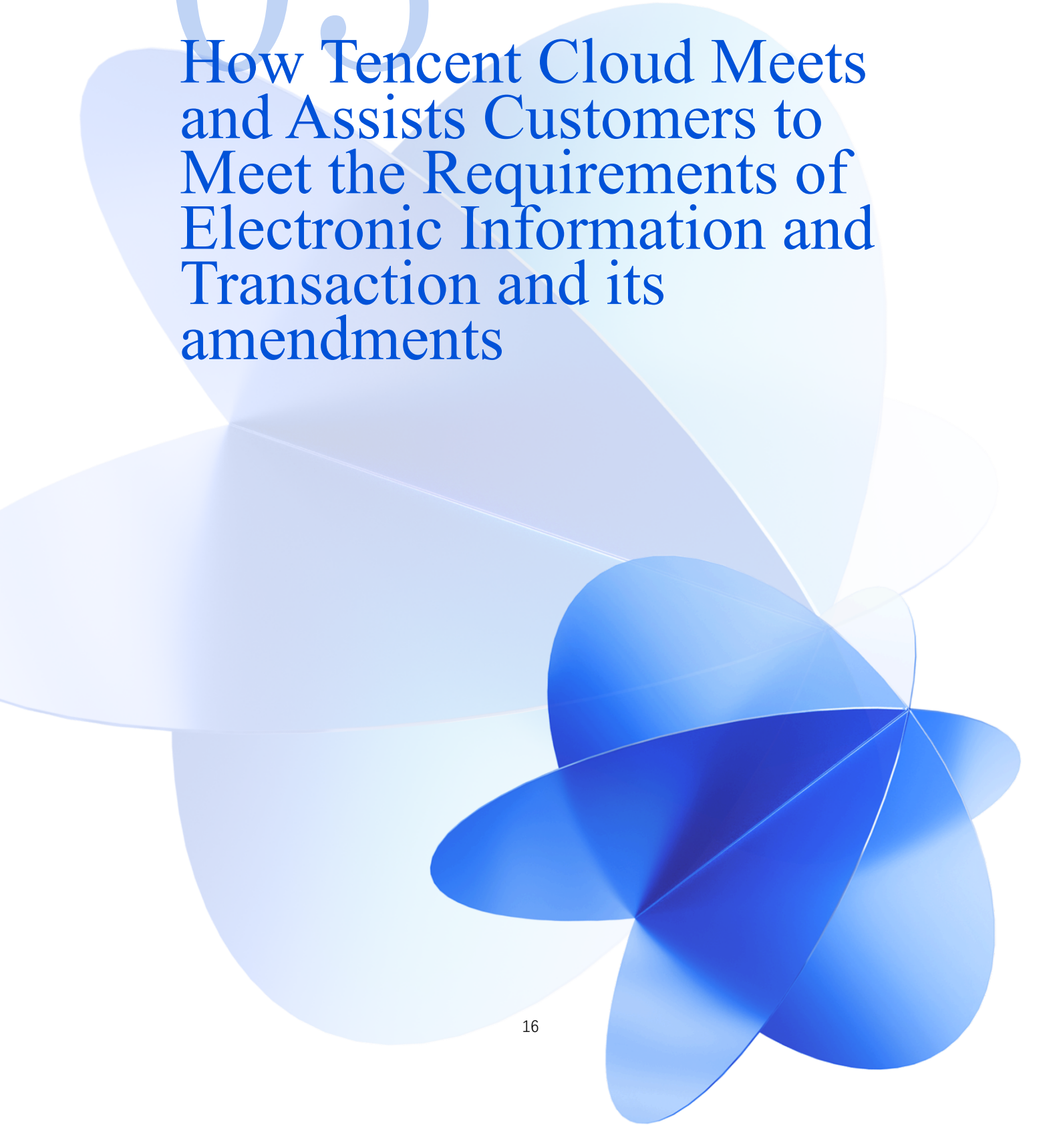
- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically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

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

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

05

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Electronic Information and Transaction and its amendments



The globalization of information has made Indonesia part of the global information community. The Government of Indonesia deems it necessary to formulate national-level regulations on electronic information and transactions to promote the development of information technology at all levels of society in an optimal, balanced, and inclusive manner, thereby enhancing the people's technological livelihood. Therefore, the Government of Indonesia Regulation No 11 Year 2008 – Electronic Information and Transaction in 2008, and amended it in 2016 by issuing Regulation No 19 Year 2016 – Electronic Information and Transaction, aiming to strengthen the legal certainty, effectiveness, prudence, and technological neutrality of the application of information technology and electronic transactions. Its provisions mainly focus on electronic information[1], electronic records and electronic signature[2], electronic certification[3], the provision of electronic system[4] , electronic transaction[5] , domain names, intellectual property rights, and privacy protection.

In this section, Tencent Cloud summarizes the control requirements in the Electronic Information and Transactions and its amendments relevant to cloud service providers, and explains how Tencent Cloud, as a CSP, assists electronic system operators[6] in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
15	Provision of electronic systems	(1) Any Electronic System Provider must provide Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems. (2) Electronic System providers shall be liable for their Provision of Electronic Systems. (3) The provision of section (2) shall not apply if it is verifiable that there occur compelling circumstances, fault, and/or	As operators of electronic systems, customers shall be responsible for the normal operation of the electronic systems they operate, and ensure their reliability and security. As a CSP, Tencent Cloud has supported millions of enterprises and individual developers with trusted cloud products and services across various sectors, including gaming, video, mobile, healthcare, public services, finance, and internet-based industries. Tencent Cloud strictly adheres to cybersecurity, user privacy, and data security laws and regulations in the jurisdictions where it operates. In keeping with the open and collaborative principles of cloud computing, Tencent Cloud

[1] Electronic information: refers to an item or a set of electronic data, including but not limited to texts, sounds, images, maps, design drawings, photos, electronic data interchange (EDI), emails, telegrams, telexes, faxes and other similar forms, as well as letters, symbols, numbers, access passwords, marks or perforations (formed after processing) that have meanings or can be understood by relevant personnel.
[2] Electronic signature: refers to electronic information that is attached, associated, or related to other electronic information and used as a tool for verification and authentication.
[3] Electronic certification: refers to certificates with electronic attributes, which include electronic signatures and identity information (used to indicate the legal status of all parties involved in electronic transactions) and are issued by electronic authentication operators.
[4] Electronic system: refers to a set of electronic devices and processes, whose functions include organizing, collecting, processing, analyzing, storing, displaying, disclosing, sending and/or disseminating electronic information.
[5] Electronic transaction: refers to a legal act implemented through computers, computer networks, and/or other electronic media.
[6] Electronic system operator: refers to any individual, state institution, enterprise, or social organization that, alone or jointly, provides goods, services, facilities, or information to users of electronic systems to meet their own or others' needs.

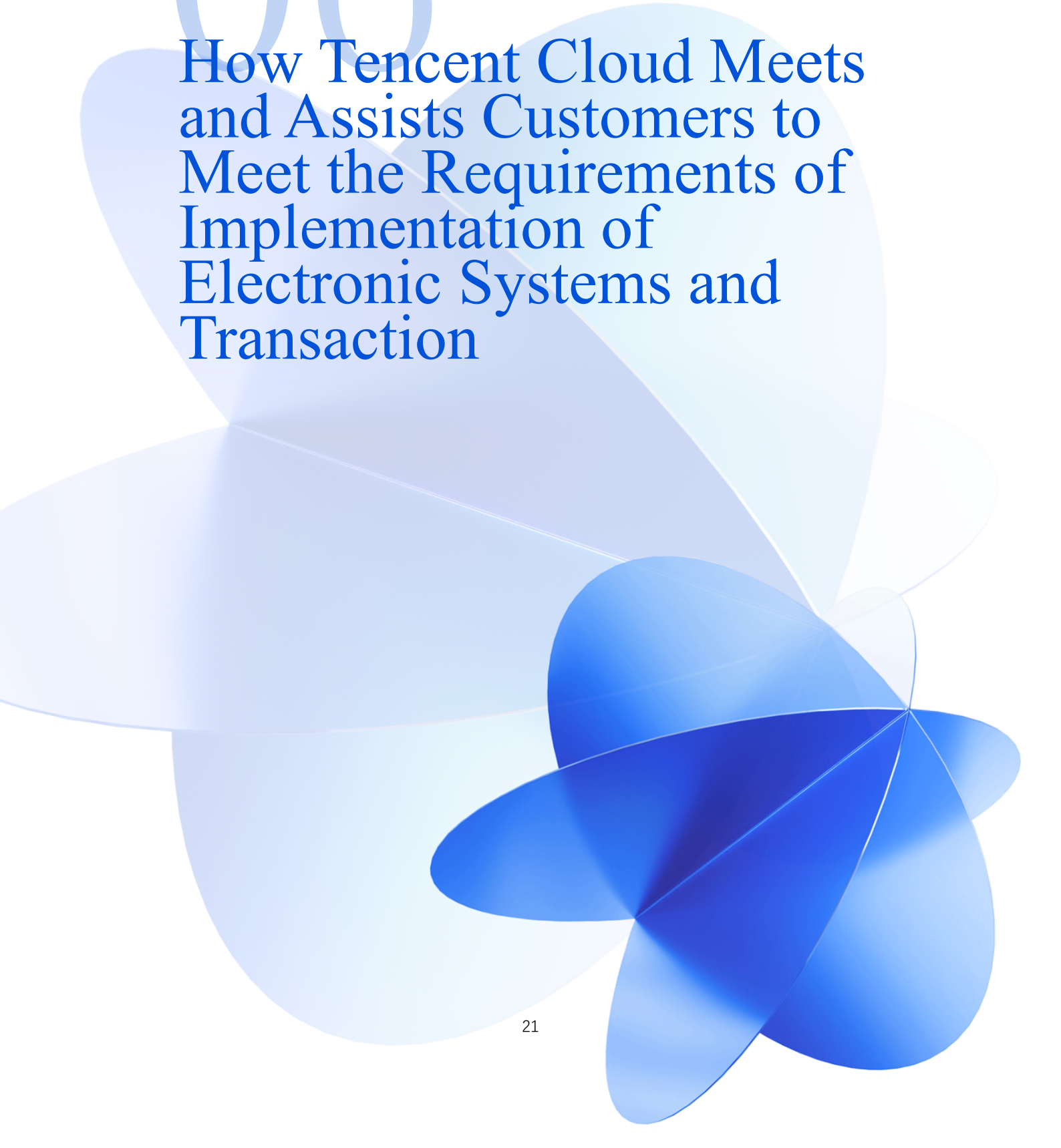
No.	Domain	Summary of Controls	Tencent Cloud's Response
		negligence on the part of the Electronic System users.	continues to enhance its cloud computing security services capabilities and work with customers to build better and more comprehensive security systems for cloud services and data. It is precisely 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. For more details, please refer to Section 3 "Tencent Cloud Security Responsibility Sharing Model". Based on this model, Tencent Cloud is committed to deepening collaboration with customers to jointly address various security challenges and ensure regulatory compliance. Tencent Cloud provides online legal documents such as **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**, which clearly define the scope of Tencent Cloud services, service levels, protection of user data and intellectual property, security responsibilities and obligations of both parties, incident and change notifications, confidentiality obligations, and information disclosure requirements. Meanwhile, the customer may choose to enter into a customized agreement with Tencent Cloud to negotiate and modify specific terms and provisions therein, thereby tailoring an agreement that complies with regulatory requirements and can obtain approval from the customer's internal procurement/legal department.
16	Operation of electronic systems	(1) To the extent not provided otherwise by individual laws, any Electronic System Providers shall be required to operate Electronic Systems in compliance with the following minimum requirements:	As operators of electronic systems, customers shall protect the availability, integrity, confidentiality, authenticity, and accessibility of electronic information during the operation of electronic systems, and clearly define the retention periods specified by law. Customers shall also provide versions of operation service descriptions in languages understandable to relevant parties and

No.	Domain	Summary of Controls	Tencent Cloud's Response
		a. able to redisplay Electronic Information and/or Electronic Records in their entirety in accordance with the retention period as provided for by the Laws and Regulations; b. able to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the provision of Electronic Systems; c. able to operate in compliance with the procedures or guidelines for the provision of Electronic Systems; d. accompanied by the procedures or guidelines that are announced in languages, information, or symbols that are intelligible to parties attributed to the provision of Electronic Systems; e. adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;	ensure the timeliness of the service descriptions. To assist customers in complying with regulatory requirements, Tencent Cloud processes customer data in strict accordance with the **Terms of Service** and **Privacy Policy** and supports customers in setting data retention periods as required by applicable laws. To ensure the confidentiality and integrity of customer data in compliance with regulatory requirements, **For data storage protection,** Tencent Cloud's storage and database products support data encryption using secure, high-strength algorithms. Encryption keys are managed through the integrated **Key Management Service (KMS)**, which provides full lifecycle management. Data is stored with multi-replica redundancy and erasure coding technology, enabling recovery measures when integrity errors are detected and significantly improving fault tolerance. **For data access and protection aspects**, customer data is classified as a high-security-level data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. Tencent Cloud has established strict access control policies and implemented permission management and authorization mechanisms. Bastion hosts are fully deployed in the production environment to centrally manage administrator account permissions and activities for backend system components. **For data backup aspects**, for customer cloud data, Tencent Cloud provides multi-replica storage and backup services according to product SLAs and assumes responsibility for backup services as agreed. If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after

No.	Domain	Summary of Controls	Tencent Cloud's Response
			the retention period expires. Deleted data cannot be restored. Tencent Cloud provides documented operational procedures and user manuals via its official website. Additionally, Tencent Cloud offers **Tencent Cloud Training and Certification** based on product knowledge and relevant professional expertise to enhance customers' technical capabilities and cloud proficiency.

06

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Implementation of Electronic Systems and Transaction



Considering that the development of information technology is essential to boost the digital economy and to safeguard the nation's sovereignty over electronic information, the Indonesian Government deemed it necessary to comprehensively regulate the application of information technology and electronic transactions. In 2019 it issued Regulation No 71 Year 2019 – The Implementation of Electronic Systems and Transaction, which provides guidance covering the operation of electronic systems, the operation of electronic agent, the conduct of electronic transactions, the implementation of electronic certification, the accreditation of trusted certification authorities, and domain-name management enabling both public sector electronic system operators and private sector electronic system operators to run their systems in a trustworthy and secure manner.

In this section, Tencent Cloud summarizes the control requirements in the Implementation of Electronic Systems and Transaction that are relevant to cloud service providers, and explains how Tencent Cloud, as a cloud service provider, assists electronic system operators in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
6	Registration of Electronic System	(1) Any Electronic System Provider must conduct registration. (2) The obligation to conduct registration for the Electronic System Provider shall be conducted before the Electronic System starts to be used by the Electronic System User. (3) The registration of the Electronic System Provider as referred to in paragraph (1) shall be submitted to the Minister through the electronically integrated business licensing services in accordance with laws and regulations.	As operators of electronic systems, customers shall complete the registration and comply with the norms, standards, procedures, etc. stipulated in the regulations. Tencent Cloud, as a CSP, has also submitted the materials required for registration to the local regulatory authorities in Indonesia and completed the registration as a private sector electronic system operator.
7	Hardware	(1) Hardware which is used by the Electronic System Provider shall: a. meet the security, interconnectivity and compatibility aspects with the used system; b. have technical support services, maintenance services,	As operators of electronic systems, customers should ensure the security, interoperability of the hardware they use, and the compatibility of the systems they employ. They are also entitled to technical support, after-sales services, etc., to ensure there is a guarantee for service continuity. To support customers in meeting regulatory requirements, **For data center security,** Tencent Cloud's infrastructure is deployed across multiple

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and/or aftersales services from the seller or the provider; and c. have a service continuity warranty. (2) The fulfillment of requirements as referred to in paragraph (1) shall be conducted through certification or other similar evidences.	global locations, organized by regions and availability zones. Each region represents an independent geographic area, and each availability zone is an isolated fault domain with physical separation. Customers can flexibly deploy data and systems across different regions or availability zones based on business growth needs and data security requirements to meet disaster recovery objectives. **For physical access control in data center**, Tencent Cloud requires operators to establish formal access procedures for data center entry, verify the identity of individuals entering the facility, and inspect and register any items brought in. Operators must regularly review access permissions to ensure proper allocation and promptly revoke any unnecessary or outdated access rights. For external visitors, Tencent Cloud mandates a visitor application and authorization process, allowing access only to approved visitors during scheduled times and under the escort of authorized personnel to designated areas. Additionally, Tencent Cloud requires operators to implement approval and inspection procedures for equipment entering or leaving the data center (e.g., installation, decommissioning, or relocation). **For hardware security and monitoring,** Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. **For computer hardware maintenance**, the relevant departments of Tencent Cloud's hardware

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management uniformly manage the hardware's work order application, acceptance confirmation, warehousing, and scheduled allocation. The demand departments shall strictly use the hardware equipment in accordance with the provisions of the instruction manual and conduct regular maintenance of the hardware equipment as required. When a hardware device breaks down, the hardware management department shall identify the nature and extent of the fault to determine whether to apply for repair. If a newly purchased computer device malfunctions during the warranty period, it shall be repaired in accordance with the regulations. An application report shall be submitted to explain the cause of the fault, and the hardware management department shall supervise the implementation. Tencent Cloud has obtained multiple security and privacy compliance certifications and qualifications through independent third-party audits or assessments, such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, and SOC, demonstrating that Tencent Cloud's security and privacy protection capabilities meet relevant certification standards and industry best practices. Tencent Cloud undergoes professional third-party audits annually. Specifically for the Indonesian region, Tencent Cloud has obtained Indonesia's SNI 27001 certification, which demonstrates Tencent Cloud's mature security management system and its ability to address evolving cyber risks in the Indonesian market.
8	Software	The Software which is utilized by the Electronic System Provider shall: a. be guaranteed of the security and reliability of proper operation; and b. ensure of the continuity of the services.	As operators of electronic systems, customers should ensure the security, operational reliability, and service continuity of the software they use. To support customers in meeting regulatory requirements, For ensuring the security of software, Tencent Cloud integrates the ISO/IEC 20000 IT Service Management Standard, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System

No.	Domain	Summary of Controls	Tencent Cloud's Response
			into the entire secure product development lifecycle. This approach covers all stages—requirements, design, development, testing, delivery, and operations—embedding information security and privacy protection principles throughout the product lifecycle to ensure robust security controls and assessments. Key security measures include: • Security Training: Promoting secure coding awareness among developers and enforcing strict adherence to secure coding standards. • Requirements Analysis: Security integration is considered during business process and technical framework discussions. • System Design: Threat modeling and security assessments are performed on system architecture. • System Development: Tencent provides secure development components for use during coding, following Tencent Cloud's secure coding guidelines. • Security Validation: Vulnerabilities are identified through code security checks, asset scans, web scans, manual security assessments, penetration testing, and code audits. • Release: Only after all high-risk issues have been fixed can the system be released to production environment to prevent vulnerabilities from being introduced into live environments. For the maintenance of service continuity and operational reliability, Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, certified to ISO/IEC 22301 international standards. To ensure service availability, Tencent Cloud conducts business impact analyses to define Recovery Time Objectives (RTO) and Recovery Point Objectives

No.	Domain	Summary of Controls	Tencent Cloud's Response
			(RPO) and develops disaster recovery strategies and continuity plans accordingly. Detailed contingency plans are established for cloud products and critical processes, and regular continuity drills are performed to validate their effectiveness. Tencent Cloud offers a ticketing service via the Tencent Cloud console, allowing customers to report faults, incidents, problems, and complaints related to security, availability, and confidentiality. In addition, Tencent Cloud provides online customer service and telephone support through the console and official website, enabling customers to report issues encountered while using Tencent Cloud services. Tencent Cloud operates multi-region redundant customer service centers that provide 24/7 support, ensuring continuous handling of customer requests, round-the-clock technical assistance for cloud products, and timely, high-quality service responses. Customers may also choose applicable service plans to access dedicated support groups, a designated technical account manager, and value-added services as part of a tailored support offering.
10	Experts	(1) Experts who are recruited by the Electronic System Provider shall have the competency in Electronic System or Information Technology. (2) Experts as referred to in paragraph (1) must comply with laws and regulations.	As operators of electronic systems, customers should ensure that background checks are conducted on the professional and technical personnel they employ, and that these personnel possess professional capabilities in the field of electronic systems or information technology. To support customers in meeting regulatory requirements, Tencent Cloud has established comprehensive human resource management standards and procedures to ensure recruitment and assignment of personnel according to job requirements. During the hiring process, Tencent Cloud will conduct background checks on candidate employees, including verifying academic qualifications, qualification certificates, etc., to ensure that their abilities are competent for the job responsibilities. Tencent Cloud has established a comprehensive training mechanism

No.	Domain	Summary of Controls	Tencent Cloud's Response
			internally, offering a variety of training courses, including compulsory training for all employees, special training for key positions, and optional professional courses, to ensure the continuous improvement of employees' professional skills.
11	Electronic System Governance	(1) The Electronic System Provider shall guarantee: a. the availability of service level agreement; b. the availability of information security agreement on the utilized Information Technology services; and c. the security of the organized information and internal communication facilities. (2) The Electronic System Provider as referred to in paragraph (1) shall ensure that any component and integrity of all Electronic System operates properly.	As the operator of the electronic system, customers shall provide a service level agreement, sign an information security agreement with the used information technology service to ensure the information security of communication facilities, and ensure the normal operation of the electronic system as expected. To support customers in meeting regulatory requirements, Tencent Cloud offers online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement**. These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud, notifications of incidents and changes, confidentiality obligations, and matters related to information disclosure. At the same time, customers can choose to sign a customized agreement with Tencent Cloud, agreeing to modify specific terms and rules in the agreement, so as to customize an agreement that complies with regulatory requirements and can be approved by the customer's internal procurement/legal department. Tencent Cloud delivers its cloud services in accordance with the agreed Service Level Agreements (SLAs). The performance indicators, measurement standards, and reporting requirements for each service are clearly defined in the SLA for the respective product and published on the Tencent Cloud official website. Tencent Cloud continuously monitors the performance and availability of its cloud services and provides real-time monitoring capabilities to

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Customers through the management console.
12	Risk management	The Electronic System Provider shall apply risk management of the occurred damage or loss.	As operators of electronic systems, customers should implement risk management to ensure that risks can be appropriately managed in a timely manner when they may cause damage or loss. To support customers in meeting regulatory requirements, Tencent has established a risk governance framework and related procedures and continuously enhances its risk management measures and internal control systems. Tencent Cloud strengthens its risk culture to effectively improve internal risk management capabilities and ensure the healthy and sustainable development of its business. Tencent Cloud has implemented a comprehensive risk management framework in accordance with ISO/IEC 27001:2022 and conducts information security risk assessments regularly, identifying risks based on risk scenarios and process analysis of business products or services. For each identified risk, Tencent Cloud evaluates its likelihood and impact, assigns a risk level, determines appropriate follow-up actions, and documents the process. Tencent Cloud also continuously monitors the status of risk treatment, assesses residual risks, and ensures that responsible parties manage risks in accordance with Tencent Cloud's risk management requirements.
13	Governance policy	The Electronic System Provider shall own a governance policy, operation work procedures, and mechanism for audit which is conducted periodically to the Electronic System.	As operators of electronic systems, customers should formulate governance policies, operational work procedures and processes, and conduct regular audits of electronic systems. To support customers in meeting regulatory requirements, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk

No.	Domain	Summary of Controls	Tencent Cloud's Response
			management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. The Tencent Cloud security team continuously monitors and assesses internal security risks to maintain the effectiveness and reliability of the information security management system. The team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to ensure a strong security posture in compliance with applicable laws, regulations, and security management standards. Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization.
14	Personal Data	(1) The Electronic System Provider must implement the principles of Personal Data protection in processing Personal Data consisting of: a. Personal Data collection is conducted in a limited and specific manner, legally valid, fair, with consent and agreement of the Personal Data owner; b. Personal Data processing is conducted in accordance with its intention; c. Personal Data processing is	As an operator of electronic systems, customers shall handle personal data in accordance with the principles of personal data protection. The processing of personal data must be based on the legitimate consent given by the data subject, and when the relevant data subject makes a request, customers shall delete the electronic information and/or electronic documents under its control that are no longer relevant. In the event of a personal data breach, customers must notify the affected data subjects in writing. To support customers in meeting regulatory requirements, **For handling personal data and personal data protection**, Tencent Cloud provides an online Privacy Policy, which clearly

No.	Domain	Summary of Controls	Tencent Cloud's Response
		conducted by ensuring the rights of the Personal Data owner; d. Personal Data processing is conducted accurately, completely, not misleading, up-to-date, accountable, and taking the intention of Personal Data processing into consideration; e. Personal Data processing is conducted by protecting the Personal Data security from loss, misappropriation, Access and illegal disclosure, as well as alteration or destruction of Personal Data; f. Personal Data processing is conducted by notifying the purpose of collection, processing activities, and failure in protecting Personal Data; and g. Personal Data processing is destroyed and/or deleted unless in a retention period in accordance with the need based on laws and regulations. (2) Personal Data processing as referred to in paragraph (1) shall consist of: a. acquisition and collection; b. processing and analysis; c. retention; d. improvement and update; e. display, announcement, transfer, dissemination, or disclosure; and/or f. deletion or destruction. (3) Personal Data processing shall comply with the provisions of a valid agreement	states that Tencent Cloud will process data in accordance with applicable laws and regulations both in the course of providing Tencent Cloud services and in any other circumstances. On this basis, Tencent Cloud regards the compliance of personal data as a primary factor in the process of service provision, and takes personal data compliance principles (such as legality, fairness, transparency, purpose limitation, data minimization, integrity, accuracy, confidentiality, accountability, etc.) as the guiding concepts for privacy compliance. These principles are integrated into all aspects of product design and development as well as the entire life cycle of personal data, making privacy compliance an inherent attribute of products. In addition, Tencent Cloud strictly abides by the privacy protection laws and regulations of all applicable countries and regions worldwide, focusing mainly on the full life cycle management of personal data, and has introduced key compliance requirements such as Privacy by Design (PbD), response to data subject rights, and disclosure of personal data. Tencent Cloud's years of security experience and accumulation ensure the security of the cloud platform infrastructure and provide a solid foundation for customers' business privacy compliance. **When obtaining the customer's consent for data processing**, When Tencent Cloud as a data controller, it collects the information provided by customers when registering for Tencent Cloud services through Tencent Cloud's official website, as well as the data generated during interactions with Tencent Cloud in this process. In such cases, Tencent Cloud will fulfill the obligations of a data controller in accordance with its Privacy Policy. When Tencent Cloud as a data processor, customers use Tencent Cloud's products or services to process data collected for their own business purposes. In such cases, Tencent Cloud is

No.	Domain	Summary of Controls	Tencent Cloud's Response
		from the Personal Data owner for one or certain purposes which have been delivered to the Personal Data owner. (4) Other than the approval as referred to in paragraph (3), the Personal Data processing shall fulfill the provisions which are required for: a. the fulfillment of contractual obligation in the event that the Personal Data owner is one of the parties or to fulfill the request of the Personal Data owner upon entering into an agreement; b. fulfillment of legal obligation from the Personal Data controller in accordance with laws and regulations; c. fulfillment of vital interest of the Personal Data owner; d. implementation of Personal Data controller authority based on laws and regulations; e. fulfillment of Personal Data controller obligation in public services for the public interest; and/or f. fulfillment of other vital interests of the Personal Data controller and/or Personal Data owner. (5) In the event of a personal data breach, the Electronic System Provider must notify in writing to the Personal Data owner.	not only responsible for the functionality and security of the products or services, but also fulfills the relevant obligations of a data processor in accordance with the Data Processing and Security Agreement. **Regarding the use, storage, and deletion of customers' personal data,** Tencent Cloud clearly specifies the purposes of various types of data collection and processing in its Privacy Policy . Tencent Cloud will not process relevant data in a manner inconsistent with these purposes. It also explains the mechanisms for retaining each type of data, sets reasonable data retention periods based on data types, and will not retain data beyond the period necessary to achieve the purposes or as required by applicable laws. If the customer informs that the purpose has been achieved or the retention period has expired, Tencent Cloud will delete the relevant customer data. Tencent Cloud has ensured the accuracy of data transmitted through Tencent Cloud by means of access control, integrity verification, and other measures. **For the response to data subjects' rights,** Under reasonable circumstances, Tencent Cloud can meet the needs of individuals (as data subjects) to delete relevant information. In addition, Tencent Cloud provides communication channels for customers. In accordance with applicable laws and regulations, it can identify corresponding data subject rights, including but not limited to the right of access, the right of correction, the right of deletion, etc., and provide applicable subject rights for data subjects, enabling customers to correct or delete relevant inaccurate data on their own. Customers can request necessary support from Tencent Cloud via email (cloudlegalnotices@tencentcom). **For security incidents that may affect**

No.	Domain	Summary of Controls	Tencent Cloud's Response
15	Personal Data	(1) Any Electronic System Provider must delete irrelevant Electronic Information and/or Electronic Document which are under their control based on the request of the relevant person. (2) The obligation to delete irrelevant Electronic Information and/or Electronic Document as referred to in paragraph (1) shall consist of: a. erasure (right to erasure); and b. delisting from search engine (right to delisting). (3) The Electronic System Provider which must delete Electronic Information and/or Electronic Document as referred to in paragraph (1) is the Electronic System Provider which obtains and/or process Personal Data under their control.	**customers**, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses.
18	Personal Data	(1) Any Electronic System Provider must provide a mechanism to delete the irrelevant Electronic Information and/or Electronic Document in accordance with laws and regulations. (2) The deletion mechanism as referred to in paragraph (1) shall at least contain provisions on: a. provision of a communication channel between the Electronic System Provider with the Personal Data owner; b. feature to delete irrelevant	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Electronic Information and/or Electronic Document which enables the Personal Data owner to delete their Personal Data; and c. recordation for the request to delete irrelevant Electronic Information and/or Electronic Document.	
19	Governance system	(1) The Electronic System Provider shall implement good and accountable governance for the Electronic System. (2) The governance as referred to in paragraph (1) shall at least fulfill the following requirements: a. the availability of procedures and guidelines in the organization of Electronic System which is documented and/or announced with a language, information, or symbol which is understood by the party who is in relation to the organization of such Electronic System; b. there is a sustainable mechanism to maintain novelty and clarity of the implementing guidelines procedures; c. there is an institutional and completeness of supporting personnel for the proper operation of Electronic System; d. there is an implementation of performance management in the Electronic System which is organized to ensure that the Electronic system operates	As operators of electronic systems, customers should establish a sound electronic system governance system with an accountability mechanism. They should ensure that there are written procedures or guidelines that are continuously updated, set up corresponding organizations and allocate sufficient personnel, and formulate plans to ensure the continuous operation of electronic systems, so as to guarantee that the electronic systems can operate as expected. To support customers in meeting regulatory requirements, **For the governance system of electronic systems,** Tencent Cloud has established an Information Security Management Policy comprising an overall security strategy, organizational structure, and management system to support secure cloud platform operations and risk management. Tencent Cloud has established a Security Technology Committee and specialized security teams across different functions and domains, supported by an experienced industry expert service team dedicated to delivering secure, reliable, professional, and compliant products and services. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		properly; and e. there is a plan to maintain the continuity of the organization of the managed Electronic System.	Tencent Cloud delivers its cloud services in accordance with the agreed Service Level Agreements (SLAs). The performance indicators, measurement standards, and reporting requirements for each service are clearly defined in the SLA for the respective product and published on the Tencent Cloud official website. Tencent Cloud provides documented operational procedures and user manuals via its official website. Additionally, Tencent Cloud offers Tencent Cloud Training and Certification based on product knowledge and relevant professional expertise to enhance customers' technical capabilities and cloud proficiency. **Regarding the sustainability of electronic systems,** Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, certified to ISO/IEC 22301 international standards. To ensure service availability, Tencent Cloud conducts business impact analyses to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and develops disaster recovery strategies and continuity plans accordingly. Detailed contingency plans are established for cloud products and critical processes, and regular continuity drills are performed to validate their effectiveness.
20	Public sector electronic system operators	(1) The public sector electronic system operators must own a business continuity plan to overcome disturbance or disaster in accordance with the risk of the impact it causes. (2) The public sector electronic system operators must conduct management, processing, and/or retention of the Electronic System and Data Electronic in Indonesian	As a public sector electronic system operators, customers formulates a business continuity plan to respond to possible disruptions or disasters. customers must manage, process, and/or store its electronic systems and electronic data within the territory of Indonesia. If the storage technology is not available within the country, it can be managed overseas only after being confirmed by a committee composed of relevant national institutions. In addition, if customers use third-party services, it must classify the data according to possible risks. To support customers in meeting regulatory

No.	Domain	Summary of Controls	Tencent Cloud's Response
		territory. (3) The public sector electronic system operators may conduct management, processing, and/or retention of the Electronic System and Electronic Data outside of the Indonesian territory in the event that the retention technology is not available domestically. (6) In the event that the public sector electronic system operators utilizes third-party services, the public sector electronic system operators must conduct data classification in accordance with the inflicted risk.	requirements, **In terms of business continuity management,** Tencent Cloud has designed and implemented a Business Continuity Management (BCM) framework tailored to its cloud environment, certified to ISO/IEC 22301 international standards. To ensure service availability, Tencent Cloud conducts business impact analyses to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and develops disaster recovery strategies and continuity plans accordingly. Detailed contingency plans are established for cloud products and critical processes, and regular continuity drills are performed to validate their effectiveness. Requirements for public sector electronic system operators to manage, process, and store data within the territory of Indonesia, Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia. The **Data Security Governance Center (DSGC)** helps customers automatically identify and classify cloud-based data assets and assess associated security risks. DSGC is an integrated data security operations platform that supports sensitive data discovery, classification and grading, data mapping, and abnormal access analysis. It works in coordination with Tencent Cloud's security capabilities to form a closed-loop data protection framework, maximizing security effectiveness for enterprises. With customer authorization, DSGC deeply integrates with various cloud data assets to obtain real-time asset information at the kernel level. Based on data characteristics, it helps identify sensitive data and organize data assets from a security perspective. Using national, industry, or enterprise-specific classification standards, DSGC assists in data classification and grading. Through visual

No.	Domain	Summary of Controls	Tencent Cloud's Response
			dashboards, customers can view the security status of assets across dimensions such as asset overview, classification, account permissions, data storage, and sensitive data. In addition, Tencent Cloud has established internal management procedures related to data security, clarifying the principles of data classification and grading as well as data protection. Customer data is classified as a high-security-level data within Tencent Cloud. Tencent Cloud employees do not attempt to access any customer data unless required for service delivery and explicitly authorized by the customer.
21	Private sector electronic system operators	(1) The private sector electronic system operators may conduct management, processing, and/or retention of the Electronic System and Electronic Data in Indonesian territory and/or outside of Indonesian territory. (2) In the event that the Electronic System and Electronic Data are managed, processed, and/or retained outside of Indonesian territory, the private sector electronic system operators must ensure the effectiveness of supervision by the Ministry or Body and law enforcement. (3) Private sector electronic system operators must provide Access to the Electronic System and Electronic Data for the purpose of supervision and law enforcement in accordance with laws and regulations. (4) Provisions on management, processing, and retention of Electronic System and	As a private sector electronic system operators, customers shall manage, process, and/or store electronic systems and electronic data either within or outside Indonesia. If the management is conducted outside Indonesia, customers shall ensure that the relevant regulatory authorities can implement effective supervision and provide the regulatory authorities with access to its electronic systems and electronic data. To support customers in meeting regulatory requirements, Tencent Cloud operates three data centers in Indonesia, providing a range of cloud computing services including cloud servers, cloud databases, and cloud storage. Indonesia-based Customers may choose to store and process their data locally within Indonesia. **Regarding customers providing access rights to electronic systems or electronic data for regulatory authorities**, Tencent Cloud offers **Cloud Object Storage (COS)**, which customers can use to store regulatory records in compliance with regulatory requirements. COS is a distributed storage service designed for storing massive volumes of files, allowing users to store and access data over the internet at any time. Customers can manage access permissions for storage buckets and objects. When a request is made for a resource, COS checks the corresponding Access Control

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Electronic Data for the private sector electronic system operators in the financial sector shall be further regulated by the regulatory and supervisory authority in the financial sector.	List (ACL) to verify whether the requester has the required permissions. Customers can create sub-accounts and assign permissions through access policies, or grant public read access to specific resources (buckets, objects, directories) to allow access by non-Tencent Cloud users. These features enable customers to provide regulatory records to regulators for inspection as required. Tencent Cloud is committed to protecting the data security of global customers and complying with the applicable laws and regulations of the countries or regions where it operates its business. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents).
22	Audit trail records	(1) Electronic System Provider must provide an audit trail for all activities of the Electronic System organization. (2) Audit trail as referred to in paragraph (1) is utilized for the purpose of supervision, law enforcement, dispute resolution, verification, testing, and other examinations.	As the operator of the electronic system, customers shall keep audit trail records of all electronic system operation activities and provide them when required by the regulatory authorities. Customers may use **Cloud Log Service (CLS)**, a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. The **Cloud Security Center (CSC)** aggregates security-related data across Tencent Cloud, including alerts from security products, asset configuration changes, user activity logs, and selected product logs. CSC provides a unified investigation platform to support comprehensive cloud log auditing and forensic analysis. Customers can also use Cloud Audit to record logs and continuously monitor account activity across

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud infrastructure. **Elasticsearch Service (ES)** enables customers to stream real-time logs from cloud servers, containers, and other cloud products, as well as ingest historical and incremental business data into Tencent Cloud ES clusters for distributed storage and analytical queries. Tencent Cloud has established comprehensive log collection and management standards covering the recording, extraction, storage, protection, analysis, and auditing of login logs, operation logs, system logs, and security event logs. All logs are centralized on Tencent Cloud's log management platform and protected with strict backup and security measures to prevent unauthorized modification or deletion. Tencent Cloud uses automated operational security auditing tools and an internal audit team to review logs regularly, detect anomalies, and mitigate operational risks.
24	Security of Organization	(1) The Electronic System Provider must own and operate procedures and facilities for the security of the Electronic System in preventing disturbance, failure, and loss. (2) The Electronic System Provider must facilitate a security system which covers the procedures and prevention and control system upon a threat and attack which causes a disturbance, failure, and loss. (3) In the event that there is a system failure or disturbance which has a serious impact as a result of other parties action to the Electronic System, the Electronic System Provider must secure the Electronic Information and/or Electronic Document and shall	As the operator of the electronic system, customers shall formulate and implement electronic system security safeguards to prevent the system from being interfered with, malfunctioning, and suffering losses. They shall also establish a security system to prevent and respond to threats and attacks. When a serious incident occurs in the system due to the actions of a third party, customers shall immediately protect the electronic information and report to the regulatory authorities as soon as possible. **To prevent the system from threats and attacks**, To implement network perimeter protection, Tencent Cloud offers the **EdgeOne (EO) platform**, which provides security and acceleration services through Tencent's global edge nodes. EO includes DDoS protection, intelligent web defense, bot/crawler attack mitigation, DNS resolution, and supports custom access control rules. Customers can also use Cloud Firewall (CFW), Web Application Firewall (WAF), and Anti-DDoS services.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		immediately report in the first place to the law enforcement and the relevant Ministry or Body.	• Cloud Firewall (CFW) provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. • Web Application Firewall (WAF) helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. • Anti-DDoS combines abundant, high-quality DDoS mitigation resources with continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks, ensuring stable and secure business operations. **To support customers in threat detection and analysis**, Tencent Cloud provides the Threat Intelligence Center (TIX), a one-stop intelligence service platform offering three core capabilities: basic intelligence, attack surface intelligence, and business intelligence. TIX supports functions such as intelligence queries, IOC analysis, and attack surface management, helping customers efficiently analyse security incidents and comprehensively assess asset exposure risks to build a robust, multi-layered security defence system. TIX aggregates intelligence from diverse sources—including vulnerability communities, security organizations, tool vendors, social media, and security blogs—and leverages cloud-based algorithms to eliminate false positives, ensuring intelligence accuracy. **For the network security protection and management within Tencent Cloud,** Tencent Cloud has established network security management standards and a defense-in-depth architecture. Tencent Cloud designs its network

No.	Domain	Summary of Controls	Tencent Cloud's Response
			security architecture based 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, development, testing 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. Empowered by TIX, Tencent Cloud aims to build a proactive defense capability framework encompassing intelligence, attack-defense, management, and planning. By integrating threat intelligence with AI and big data technologies, Tencent Cloud improves incident response speed and effectiveness and operates a 24/7 Security Operations Center (SOC) focused on threat detection, investigation, and response, ensuring security posture is visible, controllable, and actionable. **For security incidents that may affect customers**, Tencent Cloud will, after internal review, notify customers of the handling and analysis results through appropriate channels based on the scope and severity of the incident. Tencent Cloud will also provide technical support to assist customers in taking remedial measures to minimize losses.
25	Save electronic information	The Electronic System Provider must redisplay the Electronic Information and/or Electronic Document as a whole in accordance with the format and retention period which is established based on laws and regulations.	As operators of electronic systems, customers should protect the availability, integrity, confidentiality, authenticity, and accessibility of electronic information during the operation of electronic systems and clearly define the retention periods stipulated by law. **For data access and protection aspects**, customer data is classified as a high-security-level

No.	Domain	Summary of Controls	Tencent Cloud's Response
			data within Tencent Cloud. Customers retain full control over their data, and Tencent Cloud does not attempt to access or disclose customer content. Tencent Cloud has established strict access control policies and implemented permission management and authorization mechanisms. Bastion hosts are fully deployed in the production environment to centrally manage administrator account permissions and activities for backend system components.
26	Save electronic information	(1) The Electronic System Provider must maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of Electronic Information and/or Electronic Document in accordance with laws and regulations. (2) In the organization of the Electronic System which is aimed at transferable Electronic Information and/or Electronic Document, the Electronic Information and/or Electronic Document shall be unique as well as explaining its possession and ownership.	To ensure confidentiality and integrity, **in terms of data storage protection**, Tencent Cloud storage and database products support encryption using strong algorithms and integrate with the **Key Management Service (KMS)** for full lifecycle key management. Redundant storage and erasure coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors. **For data backup and storage security aspects**, For customer cloud data, Tencent Cloud provides multi-replica storage and backup services according to product SLAs and assumes responsibility for backup services as agreed. Tencent Cloud offers online legal documents such as the **Terms of Service**, **Service Level Agreement (SLA)**, and **Data Processing and Security Agreement.** These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. If customers need to terminate services due to business changes or IT planning, they can back up and migrate cloud data at any time. Upon service termination, Tencent Cloud will follow strict data erasure procedures, permanently deleting all customer data, including replicas and backups, after the retention period expires. Deleted data cannot be restored.

No.	Domain	Summary of Controls	Tencent Cloud's Response
28	User Training	(1) The Electronic System Provider must provide training to users. (2) The training content specified in Clause (1) shall at minimum cover the respective rights, obligations and liabilities of all relevant parties, as well as complaint submission procedures.	As an electronic system operator, customers shall provide training to users, covering the respective rights, obligations and liabilities of all relevant parties as well as complaint procedures, among other content. In addition, the customer shall disclose to users information including the operator's identity, system security, contractual terms, personal data protection policies and complaint channels, and clarify the rights, obligations and liabilities of all relevant parties to users.
29	Information disclosure	The Electronic System Provider must provide information to the Electronic System User at least on: a. identity of the Electronic System Provider; b. the transacted object; c. feasibility or security of the Electronic System; d. procedures for device utilization; e. contract terms; f. procedures to reach agreement; g. privacy and/or protection of Personal Data guarantee; and h. phone number of the complaint center.	To support customers in meeting regulatory requirements, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of Tencent Cloud's offerings, the protection of user data and intellectual property, the security responsibilities and obligations of both the customer and Tencent Cloud, notifications of incidents and changes, confidentiality obligations, and information disclosure matters. Customers can choose to sign a customized agreement with Tencent Cloud, negotiate to modify specific terms and rules in the agreement, so as to customize an agreement that complies with regulatory requirements and can be approved by the customer's internal procurement/legal department. Tencent Cloud's online Privacy Policy clearly informs users about the types of personal information that Tencent Cloud will collect, how the collected personal information will be used, with whom the collected personal information will be shared, where the collected personal information will be processed, how long the collected personal information will be retained, and how users can exercise their rights over their own information. Meanwhile, Tencent Cloud provides customers with training and certification programs based on Tencent Cloud product knowledge and relevant

No.	Domain	Summary of Controls	Tencent Cloud's Response
			professional competencies. It also makes cloud product operation procedures, user manuals and other materials available to customers via its official website, to enhance customers' technical capabilities and cloud proficiency.
32	Personnel training	(1) Any person who works within the Electronic Systems organization must secure and protect the facilities and infrastructure of Electronic System or information which are distributed through the Electronic System. (2) The Electronic System Provider must provide, educate, and train the personnel whose duties and responsibilities are concerned with the security and protection of facilities and infrastructure of the Electronic System.	Customers should carry out education and training for personnel in the operating environment of electronic systems to safeguard and protect the facilities and infrastructure of electronic systems, as well as the information transmitted by electronic systems. To support customers in meeting regulatory requirements, Tencent Cloud enforces access control and permission management and requires employees to sign confidentiality agreements to safeguard customer data. Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements. Tencent Cloud integrates information security management into daily operations to ensure employees understand and comply with internal policies and requirements.
33	Provide electronic information for criminal investigation	For the purpose of criminal justice process, the Electronic System Provider must provide the Electronic Information and/or Electronic Data which are contained in the Electronic System or Electronic Information and/or Electronic Data which are processed by the Electronic System at a valid request from an investigator for certain criminal act in	As operators of electronic systems, customers should ensure that when investigators make legitimate requests, they provide the electronic information or data stored in their electronic systems for criminal investigations. Tencent Cloud is committed to protecting the data security of global customers and complying with the applicable laws and regulations of the countries or regions where it operates its business. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole

No.	Domain	Summary of Controls	Tencent Cloud's Response
		accordance with the authority regulated in laws.	ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents).
34	Feasibility Test	(1) The Electronic System Provider must conduct a Feasibility Test for Electronic System. (2) The obligation as referred to in paragraph (1) may be implemented to all components or parts of components in the Electronic System in accordance with the characteristics of the needs for protection and strategic nature of the organization of the Electronic System.	As operators of electronic systems, customers should conduct feasibility tests on their electronic systems. To support customers in meeting regulatory requirements, Tencent Cloud requires that after new product development or major product changes, the testing team prepares a corresponding test plan and test cases based on product requirements and organizes a review of these test cases with the project team. Once confirmed, the testing team performs functional testing to ensure product functionality is reliable and meets Tencent Cloud's internal quality standards. After functional testing, the security team conducts security testing. Any defects or vulnerabilities identified during testing are handled according to Tencent Cloud's vulnerability management process, and the testing team issues a test report for confirmation by relevant teams.

07

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Implementation of Private Electronic System Providers and its amendments

To meet the need for regulating private sector electronic system operators and implement the relevant provisions in Regulation No 71 Year 2019 – The Implementation of Electronic Systems and Transaction issued , the Ministry of Communication and Informatics of the Republic of Indonesia formulated Regulation No 5 Year 2020 – Private Electronic System Providers in 2020. This regulation aims to govern the registration of private sector electronic system operators, the governance and content review of electronic information and/or electronic documents, the application for internet access suspension of illegal electronic information and/or electronic documents, and the granting of access rights to electronic systems and/or electronic data for the purpose of criminal supervision and law enforcement. In 2021, the Ministry of Communication and Informatics of the Republic of Indonesia issued Regulation No 10 Year 2021 – Amendment to Regulation No. 5 of 2020.

In this section, Tencent Cloud summarizes the control requirements relevant to cloud service providers in Private Electronic System Providers and its amendments, and explains how Tencent Cloud, as a cloud service provider, assists private sector electronic operators in complying with these requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
2	Private sector electronic system operator	(1) Every Private sector electronic system operator (PSE) is obliged to register. (3) The registration obligation for private sector electronic system operator must be fulfilled before the Electronic System is put into use by Electronic System Users. (4) Registration of ISPs[7] as private sector electronic system operator shall be carried out through the licensing process administered by the Ministry in accordance with laws and regulations.	As a private sector electronic system operator, customers shall complete registration and comply with the norms, standards, procedures, etc., stipulated in the regulations. As a cloud service provider, Tencent Cloud has also submitted the materials required for registration to the local regulatory authorities in Indonesia and completed the registration as an electronic system operator in the private sector.
9	Governance and moderation of electronic information and/or electronic documents	(1) A private sector electronic system operator shall be responsible for operating its Electronic System and managing the Electronic Information and/or Electronic Documents therein in a reliable, secure, and	As a private sector electronic system operator, customers shall ensure the security and stability of its electronic systems, and provide service instructions in Indonesian in accordance with legal regulations. At the same time, customers shall ensure that the electronic systems do not contain or disseminate any non-compliant information

[7] Internet access service provider: refers to a network access service operator that provides multimedia services and enables the public to connect to the public Internet.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		accountable manner. (2) Private sector electronic system operator instructions in Indonesian in accordance with laws and regulations. (3) Private sector electronic system operator shall ensure that: a. their Electronic Systems do not contain prohibited Electronic Information and/or Electronic Documents; and b. their Electronic Systems do not facilitate the dissemination of prohibited Electronic Information and/or Electronic Documents. (4) Prohibited Electronic Information and/or Electronic Documents referred to in paragraph (3) are classified as follows: a. those that violate statutory provisions; b. those that disturb the public and disrupt public order; and c. those that instruct or provide access to prohibited Electronic Information and/or Electronic Documents. (5) The specific prohibited Electronic Information and/or Electronic Documents mentioned in paragraph (4)(b) shall be determined by the relevant Ministry or Agency in accordance with laws and regulations. (6) Any private sector	and/or documents. Tencent Cloud adheres to the principles of openness and sharing in cloud computing services, continuously enhancing the security capabilities of its cloud platform and services. Together with customers, we strive to build a more comprehensive and robust security assurance system for cloud-based business and data. Tencent Cloud strictly complies with the laws and regulations related to cybersecurity, user privacy, and data security in the jurisdictions where its business operates to ensure cloud security. As a private sector electronic system operator, Tencent Cloud has provided Indonesian customers with localized language versions of its official website, service terms, data processing and security agreements, privacy policies, etc. Tencent Cloud provides the online Usage Policy .This accepted usage policy defines the rules of good conduct applicable to customers' use of Tencent Cloud. Customers must not, are not allowed to, or cause any person (including any end user) to perform any of the following prohibited activities on or in connection with Tencent Cloud (or encourage any person to engage in such prohibited activities), including violating the Tencent Cloud Service Terms; using Tencent Cloud in a manner or for a purpose that violates the Tencent Cloud Service Terms or any other service terms of Tencent's services or products; illegal, harmful or offensive use or content, as well as containing security vulnerabilities or network abuse.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		electronic system operator that fails to fulfil the obligations under paragraph (3) shall have its Electronic System access blocked (access blocking) in accordance with this Ministerial Regulation.	
10	Private sector Electronic System Operators Regarding User-Generated Content	(1) To fulfil the obligation under Article 9 paragraph (3), User-Generated-Content Private sector Electronic System Operators shall: a. establish governance policies for Electronic Information and/or Electronic Documents; and b. provide a reporting facility. (2) The governance policies referred to in paragraph (1)(a) shall at minimum contain: a. rights and obligations of Electronic System Users when using the service; b. rights and obligations of private sector electronic system operator when operating electronic systems; c. provisions on liability for Electronic Information and/or Electronic Documents uploaded by Users; and d. availability of complaint-handling channels, services and dispute-resolution mechanisms. (3) The reporting facility referred to in paragraph (1)(b) must be publicly accessible	As a private sector electronic system operator that deal with user-generated content, customers shall ensure that the electronic systems establish electronic information security governance. This includes clarifying the obligations and rights of users when using the services of the electronic systems, the obligations and rights of private electronic system operators in operating the electronic systems, the liability clauses for information/files uploaded by users of the electronic systems, as well as complaint handling and dispute resolution, among other aspects. To support customers in meeting regulatory requirements, Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of Tencent Cloud's offerings, the protection of user data and intellectual property, the security responsibilities and obligations of both the customer and Tencent Cloud, notifications of incidents and changes, confidentiality obligations, and information disclosure matters. Customers can choose to sign a customized agreement with Tencent Cloud, negotiate to modify specific terms and rules in the agreement, so as to customize an agreement that complies with regulatory requirements and can be approved by the customer's internal procurement/legal

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and used to submit complaints and/or reports about prohibited Electronic Information and/or Electronic Documents residing on the PSE's system. (4) Upon receiving complaints and/or reports under paragraph (3) regarding prohibited content, operators of electronic systems in the private sector shall: a. respond to the complainant and/or reporter; b. conduct an independent review of the complaint/report and/or request verification from the Minister or relevant Ministry/Agency; c. notify the User who uploaded the content about the complaint/report; and d. reject the complaint/report if the reported material does not constitute prohibited Electronic Information and/or Electronic Documents. (5) Any Private sector electronic system operators that fails to meet the obligations in paragraphs (1) and (4) shall have its Electronic System access blocked (access blocking) in accordance with this Ministerial Regulation.	department. **For customer-initiated reporting or inquiries**, Tencent Cloud offers a ticketing service via the official website console. This service supports reporting of issues related to security, availability, and confidentiality. The ticketing system assigns priorities through a tiered response mechanism. If frontline technical teams cannot resolve an issue effectively, the system automatically triggers an escalation process, involving product or technical teams to ensure timely resolution of customer needs or feedback. Tencent Cloud also provides online and telephone channels on its official website for customers to report issues encountered while using Tencent Cloud services. With geographically distributed customer service centres, Tencent Cloud delivers uninterrupted 24/7 support for inquiries and technical assistance. Customers may also choose service plans that include dedicated support groups, technical service managers, and value-added services for tailored assistance.
12	Cloud Computing Service Providers	(1) To fulfil the obligation referred to in Article 9 paragraph (3), Cloud	As a private sector electronic system operator, customers shall establish electronic information security governance, clarify the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Computing Operators shall establish governance policies regarding Electronic Information and/or Electronic Documents. (2) The governance policies referred to in paragraph (1) shall at minimum cover: a. the rights and obligations of users of the Cloud Computing Operator's services when utilizing cloud computing; b. the rights and obligations of the Cloud Computing Operator in delivering cloud computing operations; and c. provisions on the liability of users for storing Electronic Information and/or Electronic Documents in the cloud environment. (3) Cloud Computing Operators must provide Electronic Information and/or Electronic Data relating to their service users that is under their control, for the purposes of supervision and law enforcement.	obligations and rights of electronic system users in using electronic system services, the obligations and rights of private electronic system operators in operating electronic systems, and the liability clauses for electronic system users when uploading information/files. And for regulatory and law enforcement purposes, it shall provide the relevant regulatory authorities with the electronic information of cloud service users that it has in its possession. As a cloud service provider, Tencent Cloud is responsible for the security of the underlying data center infrastructure and the cloud platform. Recognizing that control responsibilities vary depending on the type of cloud service selected—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS)—Tencent Cloud has established a Cloud Shared Responsibility Model tailored to different service categories. For more details, please refer to Section 3 "Tencent Cloud's Shared Responsibility Model."Based on this model, Tencent Cloud is committed to deepening collaboration with customers to jointly address various security challenges and ensure regulatory compliance. Tencent Cloud offers online legal documents such as the Terms of Service, Service Level Agreement (SLA), and Data Processing and Security Agreement. These documents clearly define the scope and service levels of Tencent Cloud's offerings, the protection of user data and intellectual property, the security responsibilities and obligations of both the customer and Tencent Cloud, notifications of incidents and changes, confidentiality obligations, and information disclosure matters. Customers can choose to sign a customized agreement with Tencent

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Cloud, negotiate to modify specific terms and rules in the agreement, so as to customize an agreement that complies with regulatory requirements and can be approved by the customer's internal procurement/legal department. Tencent Cloud provides an online Usage Policy. This accepted usage policy stipulates the rules of good conduct applicable to customers' use of Tencent Cloud, clarifies customers prohibited activities, and sets restrictions on the use of Tencent Cloud software. Tencent Cloud is committed to protecting the data security of global customers and abides by the applicable laws and regulations of the countries or regions where it operates its business. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents).
13	Requests for disconnection of prohibited electronic information and/or electronic documents	(1) Private sector Electronic System Operators shall take down any Electronic Information and/or Electronic Documents that are prohibited under Article 9 paragraph (4). (2) The take-down obligation referred to in paragraph (1) includes taking down Electronic Information and/or Electronic Documents that may facilitate the dissemination of other	As a private sector electronic system operator, customers should pay attention to applications for prohibiting access to illegal electronic information submitted by the public, departments or institutions, law enforcement officers, and judicial authorities through websites/applications, emails, etc. Customers should promptly prohibit access to illegal electronic information/files. Tencent Cloud provides an online Usage Policy, which clearly states that when Tencent Cloud anticipates, considers, or suspects that a customer's Tencent Cloud account has been or may be used for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		prohibited Electronic Information and/or Electronic Documents.	unauthorized, illegal, or improper use of any Tencent Cloud services in violation of the usage policy, it may, at its own discretion, take appropriate and necessary actions, such as suspending or terminating the customer's access to Tencent Cloud and/or blocking messages or content from specific IP addresses or domains. Tencent Cloud may suspend or terminate any user's use of or access to Tencent Cloud in accordance with the Tencent Cloud Service Terms.
14	Requests for disconnection of prohibited electronic information and/or electronic documents	(1) Requests to take down (Pemutusan Akses) prohibited Electronic Information and/or Electronic Documents as referred to in Article 13 may be submitted by: a. members of the public; b. Ministries or Agencies; c. Law-Enforcement Officers; and/or d. judicial bodies. (2) Requests referred to in paragraph (1) may be delivered through: a. websites and/or applications; b. non-electronic letters; and/or c. electronic mail. (3) Requests under paragraph (1) are deemed urgent when they concern: a. terrorism; b. child pornography; or c. content that disturbs the public and disrupts public order.	
21	Granting access to electronic systems and/or electronic data for the purposes of criminal	(1) Private sector Electronic System Operators shall, in accordance with laws and regulations, grant access to their Electronic Systems	As a private sector electronic system operator, customers shall, in accordance with legal provisions, provide regulatory authorities with access to electronic systems

No.	Domain	Summary of Controls	Tencent Cloud's Response
	supervision and law enforcement	and/or Electronic Data to the relevant Ministry or Agency for supervision purposes. (2) Private sector Electronic System Operators shall, in accordance with laws and regulations, grant access to their Electronic Systems and/or Electronic Data to law-enforcement officers for law-enforcement purposes.	when required for regulatory purposes. **Regarding customers providing access rights to electronic systems or electronic data for regulatory authorities,** Tencent Cloud offers **Cloud Object Storage (COS)**, which customers can use to store regulatory records in compliance with regulatory requirements. COS is a distributed storage service designed for storing massive volumes of files, allowing users to store and access data over the internet at any time. Customers can manage access permissions for storage buckets and objects. When a request is made for a resource, COS checks the corresponding Access Control List (ACL) to verify whether the requester has the required permissions. Customers can create sub-accounts and assign permissions through access policies, or grant public read access to specific resources (buckets, objects, directories) to allow access by non-Tencent Cloud users. These features enable customers to provide regulatory records to regulators for inspection as required. **Cloud Access Management (CAM)** helps customers securely and granularly manage access to Tencent Cloud products and resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions. CAM also supports multiple secondary authentication methods, such as MFA device verification or SMS code verification, to confirm identity and environment security before login or performing sensitive operations. Tencent Cloud is committed to protecting the data security of global customers and complying with the applicable laws and regulations of the countries or regions where it operates its business. Customer data is classified as a high-security-level data within

No.	Domain	Summary of Controls	Tencent Cloud's Response
			Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents).
25	Appoint focal point	(1) Private sector Electronic System Operator shall appoint at least one focal point (Narahubung) domiciled in Indonesia to facilitate requests for access to its Electronic System and/or Electronic Data submitted by any Ministry or Agency. (2) The focal point referred to in paragraph (1) shall receive access requests concerning the Electronic System and/or Electronic Data from the focal point designated by the relevant Ministry or Agency and shall forward such requests to the Private sector Electronic System Operator.	As a private sector electronic system operator, customers shall designate at least one contact person resident in Indonesia to coordinate and handle requests from regulatory authorities for access to electronic systems and/or data. To support customers in meeting regulatory requirements, Tencent Cloud has assigned information security liaisons, who will maintain smooth communication with local regulatory authorities in accordance with compliance and business requirements, and handle requests for access to electronic systems and/or electronic data submitted for the purpose of supervision or criminal law enforcement.
30、40	Data security	(1) Access to the Electronic System provided by a Private sector Electronic System Operator is restricted and confidential. (2) Such access may only be used by officials of the Ministry or Agency designated (3) Access to the Electronic System must ensure the	The access rights to the electronic systems provided by the customer as a private sector electronic system operator shall be restrictive and confidential, and shall be used only by the regulatory personnel who have submitted applications. When granting access rights, it is necessary to ensure the integrity, availability, and confidentiality of data, as well as the reliability and security of electronic systems, and to protect the personal data within the systems.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		protection of: a. the integrity, availability, and confidentiality of Electronic Data; b. the reliability and security of the Electronic System; and c. Personal Data stored, transmitted, or processed within the system.	To support customers in meeting regulatory requirements, **In terms of personal data protection**, Tencent Cloud regards the compliance of personal data as the primary factor in the process of service provision. It takes personal data compliance principles (such as legality, fairness, transparency, purpose limitation, data minimization, integrity, accuracy, confidentiality, accountability, etc.) as the guiding concepts for privacy compliance, and integrates them into all aspects of product design and development as well as the entire life cycle of personal data, making privacy compliance an inherent attribute of products. In addition, Tencent Cloud strictly abides by the privacy protection laws and regulations of all applicable countries and regions around the world. Tencent Cloud's years of security experience and accumulation ensure the security of the cloud platform's infrastructure and provide a solid foundation for customers' business privacy compliance. Customer data is classified as a high-security-level data within Tencent Cloud. Customers retain sole ownership and control over their data content. Tencent Cloud employees will never access customer data unless required for service delivery or troubleshooting, and only with explicit customer authorization or under circumstances permitted by national laws and regulations (e.g., investigations by government authorities related to criminal incidents). To ensure confidentiality and integrity, **in terms of data storage protection**, Tencent Cloud storage and database products support encryption using strong algorithms and integrate with the **Key Management Service (KMS)** for full lifecycle key management. Redundant storage and erasure

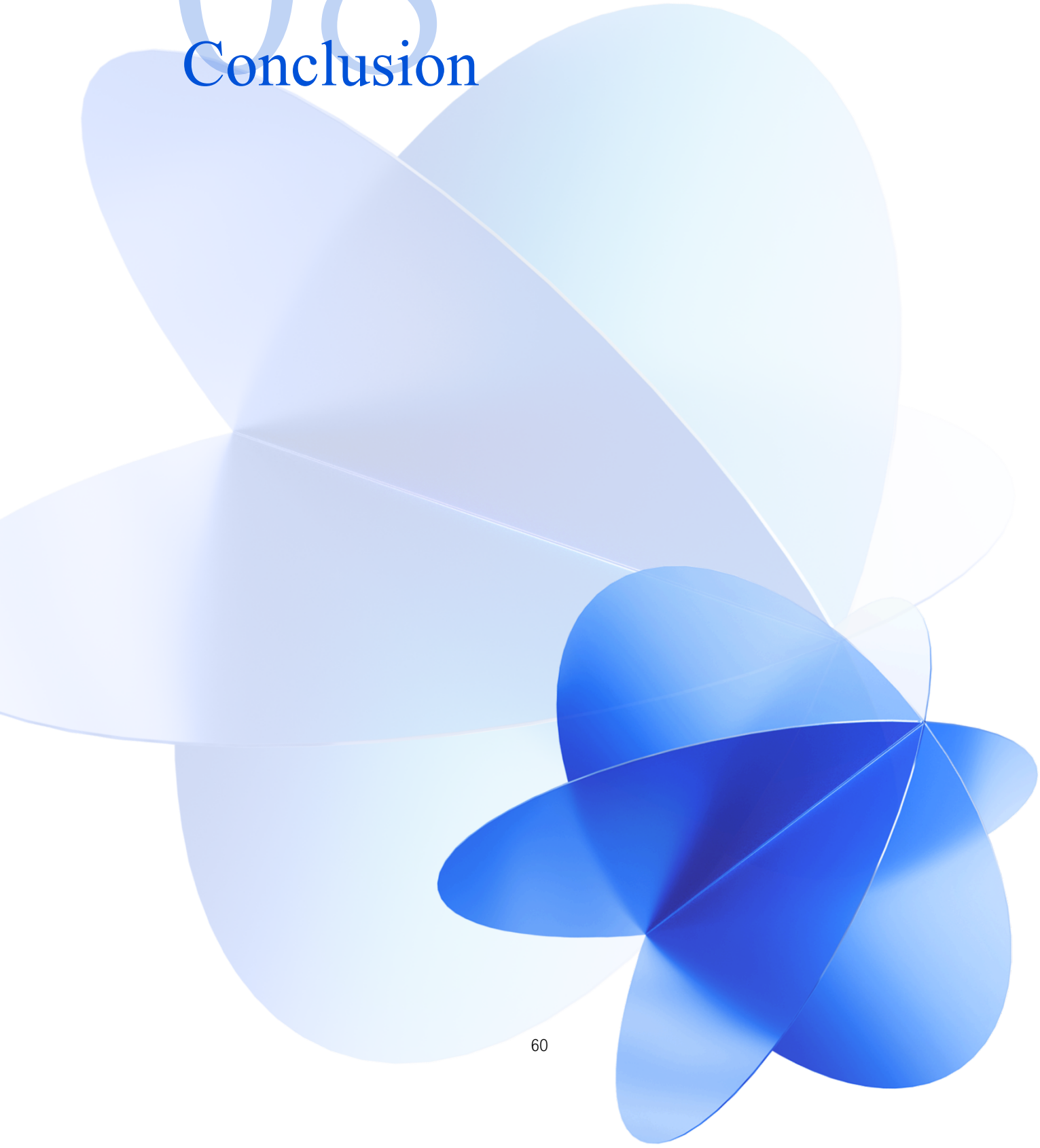
No.	Domain	Summary of Controls	Tencent Cloud's Response
			coding are used to enhance fault tolerance, with immediate recovery measures taken upon detecting integrity errors. **For data transmission protection**, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. **Regarding customers providing access rights to electronic systems or electronic data for regulatory authorities,** Tencent Cloud offers **Cloud Object Storage (COS)**, which customers can use to store regulatory records in compliance with regulatory requirements. COS is a distributed storage service designed for storing massive volumes of files, allowing users to store and access data over the internet at any time. Customers can manage access permissions for storage buckets and objects. When a request is made for a resource, COS checks the corresponding Access Control List (ACL) to verify whether the requester has the required permissions. Customers can create sub-accounts and assign permissions through access policies, or grant public read access to specific resources (buckets, objects, directories) to allow access by non-Tencent Cloud users. These features enable customers to provide regulatory records to regulators for inspection as required. **Cloud Access Management (CAM)** helps customers securely and granularly manage access to Tencent Cloud products and resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions.

No.	Domain	Summary of Controls	Tencent Cloud's Response
27、31、37、41	Request deadline	Private sector Electronic System Operator shall comply with the request within a maximum of five (5) calendar days from the date it is submitted by the Ministry or Agency's focal point (Narahubung).	As a private sector electronic system operator, customers shall provide the regulatory authority with access to electronic data within 5 calendar days upon receiving a request from the contact person of the ministry or institution. Tencent Cloud receives requests from regulatory authorities or law enforcement officers to access electronic systems and/or electronic data for the purpose of supervision or criminal law enforcement, the regional information security liaison will communicate with the regulatory authorities and cooperate with customers and regulatory authorities to fulfill the relevant requests.
42	Cloud computing service provider	(1) Cloud computing service provider shall grant access to their Electronic System and/or Electronic Data for law-enforcement purposes as referred to in Article 21(2). (2) The obligation to provide access under paragraph (1) applies only in emergency situations related to: a. terrorism; b. child pornography; c. human trafficking; d. organized crime; and/or e. life-threatening or physically injurious emergencies, in accordance with applicable laws and regulations. (3) The access obligation set out in paragraphs (1) and (2) must be fulfilled no later than five (5) calendar days from the date the request from the	As a private sector electronic system operator, customers shall, in accordance with legal provisions, provide regulatory authorities with access to the electronic system when required by regulation and only in emergency situations involving terrorism, child pornography, human trafficking, organized crime, and other threats to life and physical harm as stipulated by law. As a cloud computing service provider, Tencent Cloud, upon receiving requests from regulatory authorities or law enforcement personnel for access to electronic systems and/or electronic data for the purpose of supervision or criminal law enforcement, the information security liaisons in each region will communicate with the regulatory authorities and complete the relevant requests within the specified time limit.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		law-enforcement officer is received.	
43、44	Audit Trail of Access to Electronic Systems and/or Electronic Data for Supervision and Criminal Law Enforcement Purposes	(1) Private sector Electronic System Operators shall maintain an audit trail of access to their Electronic System by Ministries or Agencies. (2) Private sector Electronic System Operators may conduct an assessment of the impact of such access by the Ministry or Agency on: a. the quality of services it provides to its Electronic System Users; b. the protection of its Users' Personal Data; and/or c. its compliance with obligations under Indonesian laws and regulations. (3) The use of access for supervisory purposes shall be limited to a reasonable period and must be accountable.	As a private sector electronic system operator, customers must maintain audit records of access permissions to the electronic system used by regulatory authorities or law enforcement personnel and set a reasonable time limit for the granting of access permissions. Customers should also assess the impact arising from regulatory authorities' access to their electronic systems. To preserve the access records of regulatory authorities to electronic systems or electronic data,Customers may use **Cloud Log Service (CLS)**, a one-stop logging platform that supports log collection, storage, retrieval, real-time consumption, and delivery. CLS helps customers address operational monitoring, security auditing, and log analysis needs. Regarding the electronic data stored by customers in Tencent Cloud **Cloud Object Storage (COS)**, COS provides log management capabilities that record detailed access information for specified source buckets, including user-initiated actions such as uploading, downloading, deleting objects, creating or deleting buckets, and modifying bucket configurations. These logs are stored as files in a designated bucket, enabling better management of storage resources. Additionally, customers can enable real-time logging for buckets using Tencent Cloud's **Cloud Log Service (CLS)**. CLS provides minute-level reporting, real-time search, visualization, and alerting for various object operation logs. Customers can identify authorized account activities on storage buckets using timestamped logs, enabling better access analysis and rapid issue

No.	Domain	Summary of Controls	Tencent Cloud's Response
			resolution in case of anomalies. Tencent Cloud provides **Cloud Access Management (CAM)** to help customers securely and precisely manage access to Tencent Cloud products and resources. CAM also supports activity monitoring through **CloudAudit**, enabling compliance checks, operational reviews, and risk assessments for Tencent Cloud account activities.
47	Transitional provisions	Private sector Electronic System Operators governed by this Ministerial Regulation must complete registration no later than six (6) months from the date this Regulation enters into force.	As a private sector electronic system operator, customers shall register and comply with the norms, standards, procedures, etc., stipulated in the regulations. Tencent Cloud has submitted the materials required for registration to the local regulatory authorities in Indonesia and has completed the registration as a private sector electronic system operator.

08 Conclusion



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

This guide is based on key regulatory requirements issued by the Indonesian Government and the Ministry of Communication and Informatics of Indonesia (Kominfo). It aims to provide customers with a comprehensive and transparent overview of how Tencent Cloud supports compliance for cloud-hosted systems and data, helping enterprises confidently and securely migrate their systems and data to the cloud. Through this guide, Tencent Cloud seeks to assist enterprise customers in effectively meeting regulatory compliance standards while achieving digital innovation and business growth.

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

09 Version History

Date	Version	Detail
April 2026	V1.0	Initial Release