Tencent Cloud GxP Compliance White Paper

May 2022

Version 1.0

Trademark Notice:

腾讯云 is a registered trademark of Tencent Cloud Computing (Beijing) Co., Ltd.
Other trademarks, product names, and company names contained in this document, together with the products described herein, belong to their respective owners.

Disclaimer

THIS DOCUMENT MAY CONTAIN FORECASTS, INCLUDING BUT NOT LIMITED TO FORECASTS ABOUT FUTURE FINANCIAL PERFORMANCE, OPERATIONS, AND PRODUCT SERIES, AS WELL AS FORECASTS ABOUT NEW TECHNOLOGIES. GIVEN VARIOUS UNCERTAINTIES, THERE MAY BE GREAT GAPS BETWEEN THE ACTUAL RESULTS AND THE FORECASTS. THEREFORE, THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR REFERENCE ONLY AND DOES NOT CONSTITUTE AN OFFER OR COMMITMENT. TENCENT MAY REVISE OR UPDATE ANY CONTENT OF THIS DOCUMENT WITHOUT PRIOR NOTICE.

TABLE OF CONTENTS

Introduction

As the healthcare industry is booming, the complex business processes and the need to manage high volumes of medical records add difficulty to data processing and storage for organizations in the fields of pharmaceuticals, medical devices, medical software, biotechnology, and medical research, among others. As such, digital transformation has become an inevitable trend in the healthcare industry. As an innovative information and communication technology, cloud computing enables quick deployment and elastic scalability and helps organizations enhance their competitivities and flexibility while significantly lowering the total costs of software and hardware investment and maintenance. There is no doubt that cloud computing offers a viable solution to healthcare organizations.

However, healthcare organizations face multiple challenges when adopting cloud architectures or services. First, they have difficulty in ensuring the stability and security of the system on the cloud. Second, they deal with an enormous amount of sensitive patient information and need to ensure the integrity and security of patient data stored on the cloud. Third, the healthcare industry is one of the most regulated industries and is required to strictly comply with the applicable regulations and standards such as HIPAA and GxP. Therefore, healthcare organizations should give due consideration to compliance in the decision-making process. Before migrating their system and data to the cloud, they should fully understand the service levels, management process, and security compliance of the cloud service providers.

Tencent Cloud has longstanding technical expertise in cloud computing and an in-depth understanding of the healthcare industry. Tencent Cloud provides a wide range of secure, reliable, and scalable cloud services and comprehensive cloud service solutions encompassing IaaS, PaaS, and SaaS for healthcare organizations, helping them build secure cloud environment and sound cloud ecosystem and ultimately promote the digital transformation and upgrade of the healthcare industry.

Tencent Cloud knows that trust is the prerequisite for customers in the healthcare industry to migrate their system and data to the cloud with peace of mind. Based on key GxP guidelines, this white paper transparently presents how Tencent Cloud helps customers ensure the compliance of on-cloud system and data, through a robust and interconnected security protection system. The goal is to support customers in effectively meeting and maintaining GxP compliance while advancing digital upgrade and innovation-driven business development.

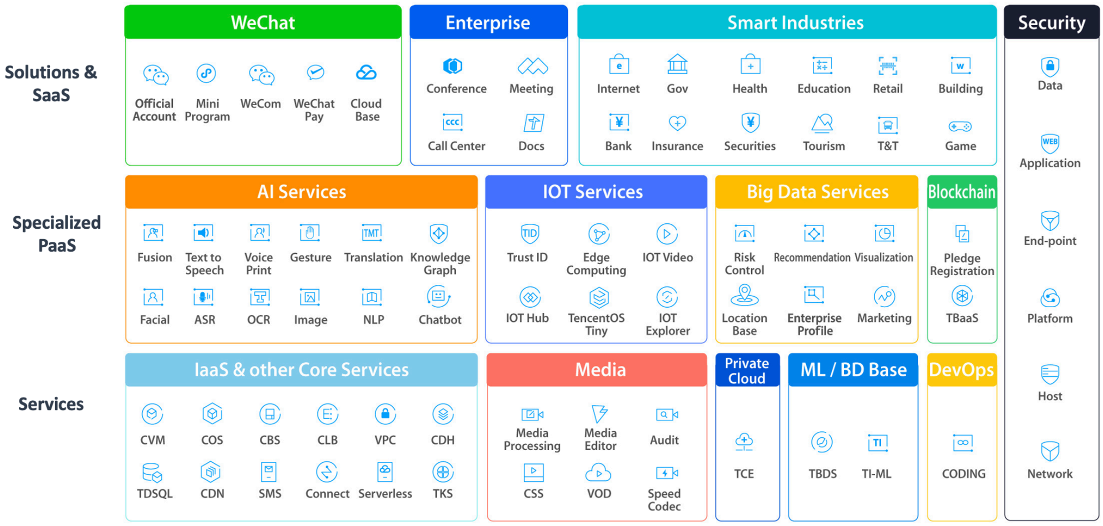
1. Tencent Cloud Overview

Tencent Cloud is a leading Chinese cloud service provider offering a wealth of world-leading products and services, such as cloud computing, AI, and big data, etc., on a worldwide basis. In the last two decades, Tencent has accumulated rich experience in the services provision through the rapid growth of its customer facing products such as QQ and WeChat. This lays solid groundwork for Tencent Cloud, serving as the technical base and connector of Tencent's internet industry. By leveraging its outstanding technical expertise, Tencent Cloud creates a wide variety of industry-specific solutions, builds an open and win-win cloud ecosystem, and empowers digital transformation in diverse sectors.

In the healthcare field, Tencent leverages its strong capabilities in open connectivity, AI, big data, cloud computing, and security to offer a suite of products such as healthcare infrastructure construction, smart healthcare, and medical AI and serve as a powerful digital assistant helping customers merge cutting-edge technologies with healthcare. Based on its industry-leading cloud computing technologies, rich service experience, and years of practice in the healthcare industry, Tencent Cloud provides a host of solutions covering multiple business scenarios, which are connected to other Tencent Cloud offerings to build an open platform. Tencent Cloud works alongside its partners to create a healthcare ecosystem covering the entire chain from medical treatment, regimen, medicine, and equipment to circulation, insurance, and services, with the aim of promoting the smart transformation of the healthcare industry.

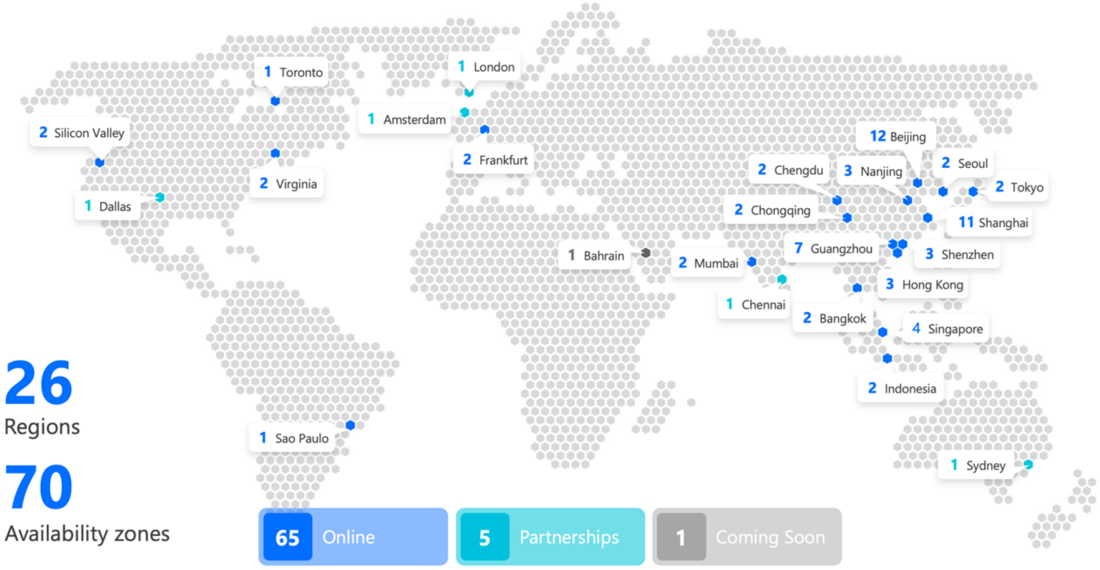
1.1 Tencent Cloud infrastructure and products

Tencent Cloud provides a full range of cloud solutions for healthcare organizations, from infrastructure to industry applications. At present, it offers over 300 products in 13 categories, covering computing, storage, database, security, big data, AI, IoT, business applications, industry applications, and developer applications.



Tencent Cloud product matrix

Thanks to its distinctive strengths in cloud infrastructure, Tencent Cloud has emerged as one of the top cloud service providers in the world. It has over one million servers and 2,800 cache nodes deployed across the globe, with storage capacity at the exabyte level and a combined peak bandwidth of over 200 Tbps. In addition, it has IDCs and operates 70 availability zones in 26 regions around the world, including the Chinese mainland, Asia Pacific, North America, and Europe, which provide customers with strong technical support.



Tencent Cloud IDC distribution chart

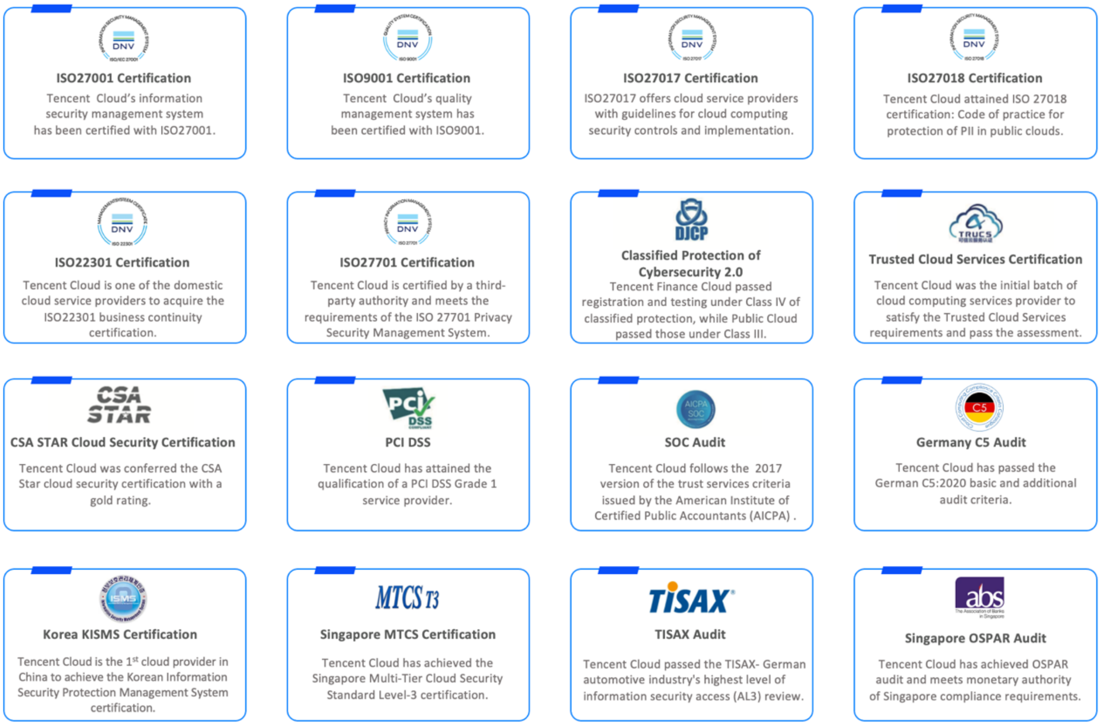
1.2 Tencent Cloud security certifications

(1) Security certifications from home and abroad

Compliance is the bedrock of Tencent Cloud's business development. In compliance with national and industry-specific requirements, Tencent Cloud is fully committed to creating trustworthy cloud services. Meanwhile, it actively participates in the formulation and promotion of industry-specific security standards and insists on compliance as a service to build and operate a secure and reliable cloud ecosystem.

In accordance with internationally recognized information security and IT management and control standards, Tencent Cloud has established the information security management system, privacy management system, quality management system, IT service management system, business continuity management system, and supply chain security management system. It provides customers with cloud services that have been reviewed and approved by authoritative third-party certification bodies. It complies with various regulatory requirements and standards in the Chinese mainland and also follows regional and industry-specific laws and regulations, standards, and best practices to continuously improve the relevant management systems, strengthen its security management, and better demonstrate its compliance practices to customers.

After third-party independent audits or evaluations, Tencent Cloud has obtained a variety of security compliance certifications or qualifications. This fully reflects that its security management meets the relevant certification standards or industry best practices. For more information, see **Tencent Cloud Compliance**.



ISO27001 Certification
Tencent Cloud's information security management system has been certified with ISO27001.

ISO9001 Certification
Tencent Cloud's quality management system has been certified with ISO9001.

ISO27017 Certification
ISO27017 offers cloud service providers with guidelines for cloud computing security controls and implementation.

ISO27018 Certification
Tencent Cloud attained ISO 27018 certification: Code of practice for protection of PII in public clouds.

ISO22301 Certification
Tencent Cloud is one of the domestic cloud service providers to acquire the ISO22301 business continuity certification.

ISO27701 Certification
Tencent Cloud is certified by a third-party authority and meets the requirements of the ISO 27701 Privacy Security Management System.

Classified Protection of Cybersecurity 2.0
Tencent Finance Cloud passed registration and testing under Class IV of classified protection, while Public Cloud passed those under Class III.

Trusted Cloud Services Certification
Tencent Cloud was the initial batch of cloud computing services provider to satisfy the Trusted Cloud Services requirements and pass the assessment.

CSA STAR Cloud Security Certification
Tencent Cloud was conferred the CSA Star cloud security certification with a gold rating.

PCI DSS
Tencent Cloud has attained the qualification of a PCI DSS Grade 1 service provider.

SOC Audit
Tencent Cloud follows the 2017 version of the trust services criteria issued by the American Institute of Certified Public Accountants (AICPA) .

Germany C5 Audit
Tencent Cloud has passed the German C5:2020 basic and additional audit criteria.

Korea KISMS Certification
Tencent Cloud is the 1st cloud provider in China to achieve the Korean Information Security Protection Management System certification.

Singapore MTCS Certification
Tencent Cloud has achieved the Singapore Multi-Tier Cloud Security Standard Level-3 certification.

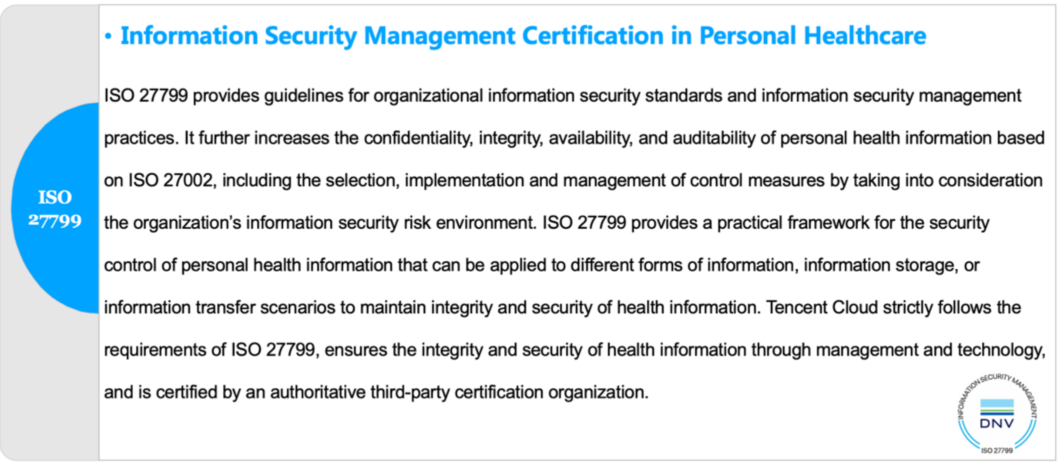
TISAX Audit
Tencent Cloud passed the TISAX- German automotive industry's highest level of information security access (AL3) review.

Singapore OSPAR Audit
Tencent Cloud has achieved OSPAR audit and meets monetary authority of Singapore compliance requirements.

Selected security compliance qualifications of Tencent Cloud

(2) Healthcare compliance certifications

Tencent Cloud has received ISO 27799 certification for personal health information protection and released the self-assessment report on compliance with the Health Insurance Portability and Accountability Act (HIPAA). With the mission to protect customer health information, Tencent Cloud strictly follows the regulatory compliance requirements, best practices, and standards of the healthcare industry:



ISO 27799

• Information Security Management Certification in Personal Healthcare

ISO 27799 provides guidelines for organizational information security standards and information security management practices. It further increases the confidentiality, integrity, availability, and auditability of personal health information based on ISO 27002, including the selection, implementation and management of control measures by taking into consideration the organization's information security risk environment. ISO 27799 provides a practical framework for the security control of personal health information that can be applied to different forms of information, information storage, or information transfer scenarios to maintain integrity and security of health information. Tencent Cloud strictly follows the requirements of ISO 27799, ensures the integrity and security of health information through management and technology, and is certified by an authoritative third-party certification organization.

2. GxP Overview

The healthcare industry plays a vital role in protecting people's health and security, hence security compliance of healthcare organizations' system and data is of paramount importance. The term GxP encompasses a broad range of compliance-related activities. It refers to a collection of regulations, guidelines, or best practices used to regulate the development, production, and sale of medical products such as drugs, medical devices, and medical software applications. The 'x' in GxP represents a particular field, such as:

- **Good Manufacturing Practice (GMP):** GMP is a system used for the authorization and control of manufacturing of products such as drugs, medical devices, and active pharmaceutical ingredients (APIs). It is intended to provide guidance for healthcare organizations to take every possible measure to ensure the quality and security of their products.
- **Good Automated Manufacturing Practice (GAMP):** GAMP can be regarded as a structured approach for the validation of automated systems. It provides guidance for healthcare organizations to adopt a flexible risk-based approach to create a compliant GxP regulated computerized system, based on scalable specification and verification.
- **Good Laboratory Practices (GLP):** GLP is intended to ensure the repeatability, consistency, reliability, and integrity of medical products by specifying the requirements for healthcare organizations in terms of risk management, management responsibility, quality management, and data integrity.
- **Good Clinical Practice (GCP):** GCP focuses on the moral aspects of clinical trials and requires healthcare organizations to follow particular protocols in clinical trials with human participants to ensure that their wellbeing, rights, and safety are not infringed.

GxP systems are formulated to comply with the quality process throughout every stage of manufacturing, storage, and distribution of medical products and to ensure the integrity of the data used to make product-related security decisions. GxP is a global standard, and each country or region has its own GxP regulators and guidelines. By comparing selected GxP standards, this GxP compliance white paper sets out how Tencent Cloud helps customers in the healthcare industry meet

GxP requirements.

Region	Standard	Description
China	Appendix 10 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China	It aims to ensure that computerized systems applied within pharmaceutical quality management processes have no negative impact on product quality, process controls, and the level of quality assurance and will not increase the overall risk.
	Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China	It aims to strengthen records and data management in drug development, production, distribution, and use processes to ensure the authenticity, accuracy, integrity, and traceability of the relevant information.
United States	Title 21 of the Code of Federal Regulations Part 11 "Electronic Records; Electronic Signatures – Application and Scope" (21 CFR Part 11) by the U.S. Food and Drug Administration (FDA)	It sets out requirements for the adoption of computerized systems to create, modify, maintain, archive, retrieve, or distribute electronic records and signatures to ensure the trustworthiness and reliability of the electronic GxP data and support GxP compliance.
	21 CFR Part 211 Current Good Manufacturing Practice	Regulations in this part contain the minimum current good manufacturing practice for preparation of drug products for administration to humans or animals. This part consists of the following subparts: Organization and Personnel, Building and Facilities, Equipment, Control of Components and Drug Product Containers and Closures, Production and Process Controls, Packaging and Labelling Control, Holding and Distribution, Laboratory Controls, Records and Reports, and Returned and Salvaged Drug Products.
	21 CFR Part 820 Quality System Regulation	This part establishes basic requirements applicable to manufacturers of finished medical devices. It outlines the regulations that govern the methods used in, and the facilities and controls used for, the design, manufacture, packaging, labeling, storage, installation, and servicing of all finished devices intended for human use. It is designed to ensure that devices are secure and effective and otherwise in compliance with other applicable regulations.
EU	Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency	This part applies to all forms of computerized systems used as part of GMP regulated activities. It aims to ensure that where a computerized system replaces a manual operation, there should be no resultant decrease in product quality, process control, or quality assurance.

3. Overview of Tencent Cloud GxP Compliance White Paper

3.1 Objectives

Based on years of deep insights into the healthcare industry, Tencent Cloud is well aware of the necessity and importance of GxP compliance for healthcare organizations. When cloud products or services are introduced into the IT environment, how to ensure compliance with GxP systems and the security and stability becomes a primary concern of healthcare organizations in the process of migrating to cloud. This GxP compliance whitepaper aims to show Tencent Cloud's compliance systems and security mechanisms to its customers in the healthcare industry, including:

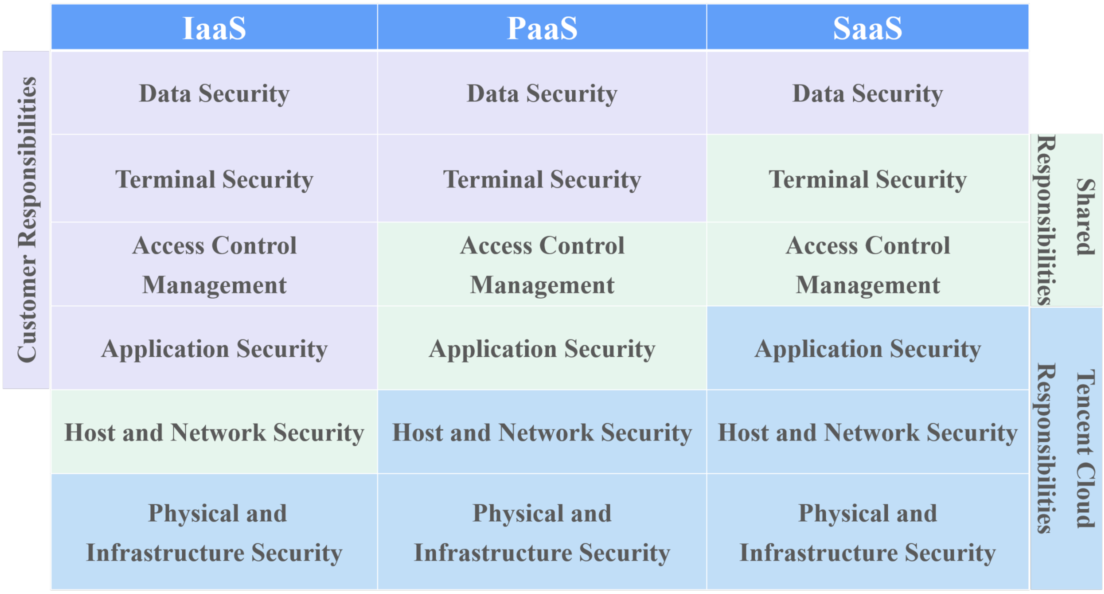
- Tencent Cloud's and customers' security responsibilities under the premise of GxP compliance;
- How Tencent Cloud's quality management system supports customers' systems in compliance with GxP requirements;
- How Tencent Cloud's management processes and technical measures help customers meet the GxP requirements for computerized systems;
- How Tencent Cloud empowers customers to assure the confidentiality, integrity, and availability of their content data stored on Tencent Cloud; and
- How Tencent Cloud's products and services help customers enhance their GxP compliance capabilities.

3.2 Target audience and scope

This white paper is targeted at GxP-regulated healthcare organizations, including but not limited to organizations in the fields of biopharmaceuticals, life sciences, medical devices, medical services, medical research, medical insurance, healthcare products, etc. Generally speaking, systems used in their GxP related activities include automated production equipment systems, automated laboratory equipment systems, laboratory information management systems, manufacturing execution systems, warehousing and distribution systems, as well as systems for the management of man, machine, materials, methods, and mother nature (5Ms), production execution and management, and quality management. If customers plan to migrate their GxP systems to the cloud, this white paper provides with information on Tencent Cloud's quality management system and security controls, so that customers can get a better understanding of how Tencent Cloud could help ensure GxP compliance. From a cloud service provider's perspective, this white paper elaborates on how Tencent Cloud helps customers meet the GxP requirements through relevant management processes, technical measures, and services. It does not cover how the GxP systems built on Tencent Cloud can meet the GxP standards such as material purity, equipment and processes, or environmental requirements, which falls within customers' responsibility to fulfill the relevant requirements in their business processes.

3.3 Shared responsibility model

Through a unified underlying architecture and resource sharing model, Tencent Cloud provides various resources such as network, storage, and computing for customers. Customers in healthcare industry can choose Tencent Cloud's IaaS, PaaS, and SaaS services as needed. Based on information assets and product features, Tencent Cloud has established the shared responsibility model in terms of information security as shown below. The sections in light blue represent Tencent Cloud's responsibilities, those in light purple represent customers' responsibilities, and those in light green represent the responsibilities shared between customers and Tencent Cloud. For more information on the shared responsibility model, see **Tencent Cloud Security White Paper.**



IaaS	PaaS	SaaS
Data Security	Data Security	Data Security
Terminal Security	Terminal Security	Terminal Security
Access Control Management	Access Control Management	Access Control Management
Application Security	Application Security	Application Security
Host and Network Security	Host and Network Security	Host and Network Security
Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security

Tencent Cloud shared security responsibility model

Given the characteristics of cloud computing, the compliance of the customers' GxP system built on Tencent Cloud is the responsibility shared between customers and Tencent Cloud. As the owner of the GxP systems and the target of industry regulation, customers should bear the ultimate responsibility for compliance of their GxP systems and related business activities. In addition to ensuring that their business processes comply with GxP standards, customers also need to ascertain that the cloud service provider for such systems also enables the GxP compliance. Tencent Cloud is a leading cloud service provider for healthcare organizations. Based on the aforesaid shared security responsibility model, Tencent Cloud is committed to providing a GxP-compliant underlying cloud platform, and helping customers build GxP-compliant business systems. According to the category of cloud services used by customers, Tencent Cloud offers reliable infrastructure and cloud products, to ensure that the components it provides meet the security requirements for GxP computerized systems. Meanwhile, customers in the healthcare industry need to select appropriate cloud products and services from Tencent Cloud according to business needs and processes, to develop and manage GxP-compliant business systems.

In order to give customers a better grasp of the security mechanisms and compliance capabilities provided by Tencent Cloud, this white paper sets forth compliance in terms of **quality management, operations and maintenance and electronic records and data management** based on the GxP standards applicable to Tencent Cloud.

4. Quality Management

4.1 Quality management system

According to GxP regulatory requirements, healthcare organizations need to establish and maintain quality management system, including quality policies, quality management structures, quality plans, and related processes. They need to develop a quality management system in alignment with their quality objectives and business processes, formulate quality policies, and set up quality management organizations. They also need to carry out management reviews on a regular basis to ensure the effective operations of the quality management system.

Tencent Cloud is one of the first cloud service providers in China to get ISO 9001 certified. It obtained the quality management system certification issued by a third-party international certification agency in 2015, and was accredited by both the China National Accreditation Service for Conformity Assessment (CNAS) and the ANSI National Accreditation Board (ANAB).

In strict compliance with the ISO 9001: 2015 standards and in light of its current conditions, Tencent Cloud has put in place a comprehensive quality management system encompassing the quality management manual, policy, objectives, as well as standards and procedures for quality management. As a systematic guide and standard for product quality management and daily operations, the system takes care of the whole process of products and services from planning, design and development, and quality control to quality assurance, aftersales service, and quality improvement, ensuring the effective implementation of its quality management measures.

4.2 Quality management audit

According to Article 4 of Appendix 1 "Computerized System" to Good Manufacturing Practice for Drugs issued by the National Medical Products Administration of China (NMPA), healthcare organizations should provide documents concerning the supplier quality system and audit information based on the risk assessment results. In order to ensure the applicability and effectiveness of its quality management system, Tencent Cloud has implemented the procedures to carry out regular performance measurement, internal and external audits, and management reviews of its quality management system. The goal is to ensure that the quality management system is aligned with its quality policy and objectives and meets customer demand for GxP compliance.

1） Quality management system effectiveness measurement and evaluation

As permitted by law, Tencent Cloud monitors and gathers relevant data from business activities. It analyzes information on customer satisfaction status and trends, alignment of products and services with customer needs, the performance of external suppliers, system operations, and so forth to comprehensively evaluate the suitability and effectiveness of the quality management system.

2） Internal audit and management review

Tencent Cloud carries out an internal audit annually to verify whether its quality management system meets the specified requirements and whether the measures taken in response to the risks and opportunities are effective. For issues revealed in the audit, Tencent Cloud will request the responsible persons to remediate the problems in a timely manner, and verify and record the implementation and effectiveness of the corrective measures taken in follow-up audits. The results of each internal audit are presented to management for review.

Tencent Cloud carries out a management review of its quality management system annually to ensure its ongoing suitability, adequacy, and effectiveness, as well as alignment with the company's overall strategies. The management review assesses the opportunities for improvement and the need for changes to the quality management system, including the quality policy and objectives.

3） Third-party audit

A third-party accounting firm is hired to assess the design adequacy and implementation effectiveness of Tencent Cloud service system security controls and issue a report every six months in accordance with the relevant regulations of the American Institute of Certified Public Accountants (AICPA). Through the System and Organization Controls (SOC) report attestations, Tencent Cloud keeps user organizations, independent auditors, regulators, shareholders, and other stakeholders informed of its latest internal controls. Additionally, Tencent Cloud asks an independent third-party certification agency to oversee and audit its ISO 9001-certified quality management system annually to ensure the compliance and effectiveness of the system.

For more information on Tencent Cloud's ISO 9001 certification and SOC audits, you can visit the Tencent Cloud Compliance Center section on Tencent Cloud official website. You can also submit a ticket or contact online customer service to view the ISO 9001 certificate and SOC reports.

4.3 Document management

According to the applicable GxP standards, regulated healthcare organizations should establish and maintain procedures for adequate control of the distribution, use of, access and revision to their internal documents. Healthcare organizations need to put in place a document management procedure to regulate the standard operating procedures (SOPs) and the procedures regarding system operations and maintenance to ensure the accuracy and effectiveness of documents.

Tencent Cloud has established a document management procedure covering all stages from document preparation, approval, release, storage, use, and revision to retention and invalidation. This procedure is designed for unified management of documents across various management systems such as quality management, cloud security management, IT service management, and business continuity management. Tencent Cloud documents can only be released after being reviewed and approved by competent persons. The approved documents will be published on the electronic document management platform, and access permissions will be granted based on the roles and responsibilities of internal personnel. Document users can only view relevant documents through the electronic document management platform and are not allowed to modify or perform other operations on the documents.

According to Tencent Cloud's document management requirements, document administrators must review and maintain relevant documents on a regular basis or when any changes occur in the company's organizational structure or business operation processes. In that case, the persons who edited the documents need to indicate the changes in the Document Change Log and submit it to the competent person for approval, so as to ensure that any revisions and changes to the document are approved, and the audit trails are kept.

4.4 Personnel management

According to GxP standards, personnel engaged in various activities throughout the lifecycle of computerized systems, such as verification, use, maintenance, and management, should receive training on the use and management of such systems according to their responsibilities and permissions to ensure that they have appropriate qualifications and capabilities to perform the assigned tasks. Therefore, cloud customers need to make sure that their business process owners, business system owners, system development, operation and maintenance (Ops) personnel, and system users collaborate with each other and receive training and guidance on the design, verification, installation, and operations of computerized systems on a regular basis. This aims to ensure that they can securely and correctly use the computerized systems to perform their duties, and promptly deal with the potential faults or failures at work.

If customers in the healthcare industry wish to digitally transform their existing IT infrastructure and systems by using cloud services, their personnel need to be equipped with the technical capabilities required for cloud services in order to minimize risks while carrying out business operations and projects on Tencent Cloud. Based on years of experience in the cloud industry, Tencent Cloud Training and Certification Center provides a step-by-step technical training certification system and a variety of special training resources, covering cloud development, cloud operations and maintenance, cloud architecture, and other fields, to help customers build a cloud training system .

Tencent Cloud has established and implemented comprehensive employee training system and process to ensure that its employees receive adequate job-specific operating procedure training, technical training, and information security awareness training before and during their employment, including office security, secure coding specifications, and security incident handling. For personnel (such as those engaged in product R&D, Ops, product operations, and aftersales support) who deal with customer data and derived data (such as customer registration information, purchase history, user log information, monitoring data, aftersales ticket records, and billing information), Tencent Cloud provides information security awareness and skills training for them to ensure that they process customer data securely, legally and in accordance with Tencent Cloud's data management requirements.

Tencent Cloud has established a security organizational structure to regulate the effective operations of the security management team, push forward the implementation of various cloud security tasks, and reduce security risks. In terms of personal information protection, Tencent Cloud has set up a dedicated privacy and data protection department and appointed the person in charge of privacy protection to promote the planning and implementation of the privacy compliance tasks.

4.5 Supplier management

According to the regulatory compliance requirements for suppliers and service providers under 21 CFR Part 820 Quality System Regulation and Title 3 "Suppliers and Service Providers" of Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP, healthcare organizations need to develop an operating procedure to manage suppliers of the computerized systems to ensure that the service providers are adequately evaluated and the computerized systems and the services they provide meet the quality requirements set forth in the service agreements.

(1) Supplier evaluation

Healthcare organizations are obliged to adequately evaluate potential cloud service providers and retain the records of evaluation. In the evaluation process, healthcare organizations need to consider key factors such as the cloud service providers' capabilities and reliability to meet specific requirements, including but not limited to quality, security, and data protection requirements. Moreover, they need to learn about and comprehensively assess the cloud service providers' reputation, compliance, etc.

Tencent Cloud has established stringent supplier evaluation and selection processes. When a new supplier is needed, Tencent Cloud's procurement department and the requesting department will comprehensively evaluate the potential suppliers' product delivery qualifications and capabilities, technical levels, quality assurance capabilities, performance in the industry, as well as risk management and governance processes. They will select potential suppliers depending on how they match the demands, and then nail down the best fit. In addition, Tencent Cloud supervises and manages its suppliers and regularly inspects their contract performance and SLA compliance. For suppliers evaluated with high-risk, Tencent Cloud will take appropriate measures to mitigate their negative impact on or risk to its business continuity.

(2) Supplier agreement

According to the guidelines from 21 CFR Part 11 "Electronic Records; Electronic Signatures – Application and Scope", regulated healthcare organizations that deal with sensitive data such as those from clinical investigations with the help of cloud service providers need to assess whether the cloud service providers have sufficient controls in place to ensure data reliability and confidentiality, and to enter into service agreements with the cloud service providers.

In general, Tencent Cloud signs a master service agreement and a service level agreement with customers. The two agreements and other binding terms and conditions on Tencent Cloud's website mainly contain the following contents: service details (including the scope, regions, and validity period of the service), service level, data storage area, protection of confidential data, Tencent Cloud's responsibilities, the customer's responsibilities, security incident notification and communication mechanism, audit permissions, and the dispute settlement mechanism. Customers can choose to sign an offline agreement with Tencent Cloud, of which the specific terms and conditions can be agreed on through negotiations between the legal departments of both sides.

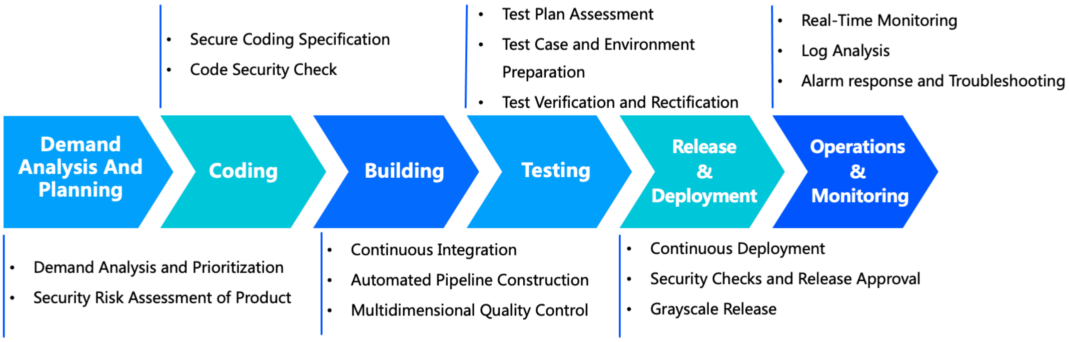
The Privacy Policy and Data Processing and Security Agreement available on Tencent Cloud's website specify the obligations of Tencent Cloud and customers with respect to data processing. They describe how Tencent Cloud employs data security technologies and security management measures to ensure the security of customer data in the processes of use, storage, disclosure, and transfer, etc. According to the agreement entered into between Tencent Cloud and the customer, customer data will be retained for a reasonable period of time after the expiration or termination of the service. The customer must migrate their data before the end of the retention period; otherwise, the data will be deleted automatically at the expiry of the retention period. 21 CFR Part 820 "Qualify System Regulation" of the Code of Federal Regulations by the U.S. FDA states that "Purchasing documents shall include, where possible, an agreement that the suppliers, contractors, and consultants agree to notify the manufacturer of changes in the product or service so that manufacturers may determine whether the changes may affect the quality of a finished device." According to the Tencent Cloud Service Agreement, Tencent Cloud will timely inform the customers of the changes to the following products or services:

- For routine maintenance (such as overhaul, maintenance, upgrade, and optimization) of the service platform or related devices, systems, and software, Tencent Cloud will notify the customers at least 24 hours in advance. Tencent Cloud will also timely inform them of non-routine maintenance for any reasons attributable to ISPs (Internet Service Providers) or force majeure.
- For major changes such as IDC relocation and device replacement, Tencent Cloud will notify the customers 30 days in advance and seek support from them.
- In case of any adjustment or termination of part or all services due to Tencent Cloud's operating arrangements, Tencent Cloud will inform its customers of such adjustment or termination at least 30 days in advance, so that the customers can take appropriate measures such as data transfer, backup or business adjustment. This effectively protects the customers' legitimate rights and interests.

4.6 System development lifecycle

According to GxP standards, healthcare organizations which adopt computerized systems need to develop and implement specific procedures and standard operating procedures throughout the lifecycle of computerized systems from request to termination, including design, standard setting, programming, testing, installation, operations, and maintenance. This aims to ensure that the use of computerized systems does not have any negative impact on the quality control and risk management of the GxP systems. When the healthcare organizations build their own cloud based GxP system, they need to ensure that the cloud vendor has implemented strict system design and development processes to achieve the overall security compliance of the GxP computerized systems. Tencent Cloud is committed to continuously improving its cloud computing service capabilities and gaining customer trust through quality assurance and secure and reliable products and services. This philosophy is embedded into every phase of system and product development and operations, giving rise to Tencent Cloud's distinctive DevOps model.

Focusing on Continuous Integration (CI) and Continuous Delivery (CD), the DevOps model aims to quickly implement system development and changes while maintaining system quality, stability, and availability. The DevOps model of Tencent Cloud integrates development, operations, quality management, and security related methods, tools, and platforms, and promotes effective communication and collaboration between R&D, Ops, quality, and security teams to respond faster to customer demand and continuously deliver services and value to customers. The model involves the following phases.


Secure Coding Specification
Code Security Check
Test Plan Assessment
Test Case and Environment Preparation
Test Verification and Rectification
Real-Time Monitoring
Log Analysis
Alarm response and Troubleshooting
Demand Analysis And Planning
Coding
Building
Testing
Release & Deployment
Operations & Monitoring
Demand Analysis and Prioritization
Security Risk Assessment of Product
Continuous Integration
Automated Pipeline Construction
Multidimensional Quality Control
Continuous Deployment
Security Checks and Release Approval
Grayscale Release

Tencent Cloud system development lifecycle

(1) Requirements analysis and planning

Tencent Cloud organizes development of new requirements or iteratives through Tencent Agile Product Development (TAPD) platform. The product team performs a detailed analysis of the collected requirements and prioritizes them on the TAPD platform. In the phase of requirements analysis, in addition to the feasibility analysis, the product team also takes into full account security issues to reduce security risks attributable to unreasonable requirements or incomplete considerations. The requirements document for Tencent Cloud products and services should incorporate security design based on internal security principles and security checklists, including the requirements for communication security, API security, permission control, data and privacy protection, audit log retention, and security compliance. Passing a formal requirements review is the prerequisite for entering into the next phase of development. The product team also needs to conduct a comprehensive security risk assessment on the overall architecture and service process of the product and lay out a clear response plan for the identified risks in a push for the resolution of the problems.

(2) Coding

In the coding phase, Tencent Cloud has secure coding specifications and coding guidelines for different programming languages and coding scenarios. The Tencent Cloud product development team needs to attend security trainings to improve their awareness and skills of secure coding. Before the testing process starts, the Tencent Cloud security team will perform a code security inspection and analysis through integrated code security inspection tools. Tencent Cloud's code security inspection and analysis solution integrates multiple capabilities such as static application security testing (SAST), open-source component detection, and sensitive information detection. Sensitive information or security vulnerabilities in the code can be detected through code scanning and third-party component security inspections to reduce security risks.

(3) Building

Tencent Cloud uses a code tool platform to ensure continuous build and has a dedicated engineering performance team for pipeline construction. Through automated code inspection, unit testing, and compilation, Tencent Cloud greatly alleviates the workload of its developers and continuously improves the code quality and development efficiency. In addition, the development, integration, and other pipelines are subject to multi-dimensional quality controls, so that they can meet the quality and time requirements during operations.

(4) Testing

Tencent Cloud has established strict testing procedures and management practices. Before the testing process starts, the person in charge needs to conduct a review and security assessment on the technical scheme and prepare the security test cases and test environment. During the test, the testing team needs to verify the test requirements checklist as shown below according to the test specifications. If any functional or security risks are identified, corrective measures must be taken. The testing phase can be completed and test reports be output only when the test results meet the quality standards for release.

- The features of the product or service function properly;
- The performance of the product or service (such as response time and concurrent processing capability) can meet the applicable requirements;
- The product has passed various security tests conducted by the security team;
- The product or service can function stably for a long time, with no abnormalities detected;
- An abnormality in a single node does not affect the overall availability of the product or service.

(5) Release and deployment

Tencent Cloud has a release process that can streamline continuous deployment. This allows for full-process management of products and services in different cluster environments, including release process management and rapid rollback. In this phase, the product team needs to ensure that the new products have been connected to Tencent Cloud Web Application Firewall (WAF) or other security tools and passed the internal penetration test, server security test, pre-release scanning, security test, system vulnerability scanning, and other security checks. Grayscale release can be implemented only with the approval of relevant teams such as product, R&D, testing, security, and Ops.

(6) Ops and monitoring

For Tencent Cloud products, services and the supporting platforms, It is required that logs of their related components should be retained and uploaded to the monitoring system. Real-time monitoring and smart data analysis of the system log data and metric information are conducted to quickly detect abnormalities, send alarms, and troubleshoot issues. For more information on the Tencent Cloud system operations and monitoring, see Section 5 "Operations and maintenance".

4.7 Validation

According to the requirements of "Electronic Records; Electronic Signatures – Application and Scope" 21 CFR Part 11 Section 11.10(a), validation of the computerized systems is required to ensure their accuracy, reliability, and conformity with the expected performance. Validation refers to the practice of checking and providing objective evidence to make sure that the specific requirements are met. In principle, healthcare organizations ought to ensure that their GxP systems are validated and function accurately as expected. In the context of cloud services, customers need to affirm that the infrastructures or cloud services provided by the cloud service provider have undergone rigorous validation and meet the SLA requirements. Based on GxP requirements, Tencent Cloud will in the following explain on how it ensures that its products and services fulfill the defined intended use and service level or help healthcare organizations achieve GxP compliance:

1) Ensuring that Tencent Cloud implements system design, development, and testing in alignment with the software development lifecycle

Tencent Cloud has developed the DevOps management model and embedded application and infrastructure security into every phase of the software development lifecycle, including requirements analysis and planning, coding, building, testing, release and deployment, as well as Ops and monitoring. Throughout the lifecycle of system development, it carries out continuous testing and security hardening based on the risk assessment results to ensure that the features and performance of the system meet user needs and quality requirements. For more information, see Section 4.5 "System development lifecycle".

2) Ensuring that the Tencent Cloud platform meets the requirements for quality management and security controls

As a leading cloud service provider, Tencent Cloud is committed to providing stable and reliable cloud products and services and standard-compliant supporting infrastructure for customers in the healthcare industry. Tencent Cloud complies with the compliance requirements in different countries and plans and creates cloud services in accordance with internationally recognized information security and IT control standards and the regulations, standards, and best practices in various regions and industries.

Tencent Cloud has established a sound risk management process. In accordance with cloud security standards and best practices, it carries out cloud security risk identification, analysis, handling, and continuous monitoring of cloud platforms (including products, services, and supporting systems, hardware, and infrastructure) every year, so as to ensure that the risks associated with Tencent Cloud assets are under control.

Tencent Cloud is subject to various external audits every year, including the ISO series certification, the Multi-Tier Cloud Security (MTCS) Standard for Singapore, the German Cloud Computing Compliance Controls Catalog (C5), the Korea Information Security Management System (K-ISMS), and SOC 2 Type II. Among them, Tencent Cloud SOC 2 is an external audit for attestations conducted by a third-party international audit agency every six months. The audit covers IDCs, supporting infrastructure, and products provided by Tencent Cloud, which evaluates the design adequacy and operational effectiveness of Tencent Cloud's internal controls (covering security, availability, stability, process integrity, and confidentiality, etc.).

3) Ensuring that Tencent Cloud components are modified in a controlled manner

Tencent Cloud has developed a strict change management procedure for components and implemented targeted management for various types of changes through a dedicated change management platform, with the aim of ensuring the systematic implementation of the change management process through tools. Changes to Tencent Cloud products, services, and supporting systems need to undergo rigorous validation before final release in order to ensure the quality of change release:

- Confirming that the use cases validation of the features meet the expectations;
- Confirming that the network traffic, logs, and monitoring metrics of the production environment are normal;
- Verifying that the API call requests in the production environment are executed properly; and
- Conducting critical path regression verification for legacy functionality that may be affected.

5. Operations and Maintenance (Ops)

5.1 Data backup and restoration

In order to ensure data availability and integrity, the GxP-regulated healthcare organizations are required to periodically back up relevant data and verify the integrity and accuracy of the data and the data restoration capabilities during the validation process, to ensure that the retention period of the backup data meets the requirements for records retention. Customers in healthcare industry need to determine the scope of data to be backed up, the backup frequency, and the backup storage method based on the business risk assessment results. If they plan to migrate the data to the cloud, they can select a data backup service according to the features of the different cloud products or services.

Tencent Cloud backs up the collected and processed data according to applicable laws and regulations. Based on the features of its products or services, Tencent Cloud provides multiple storage replicas and backup services in accordance with the product documentation or SLA, and takes responsibility for the data backup services provided within the agreed scope. If the customers have purchased and configured the data backup service provided by Tencent Cloud and want to get more information, they can submit a ticket to Tencent Cloud to get the following information:

- The scope and schedule of data backup
- The storage location and retention period of backup data
- Procedure for validating the integrity of backup data
- Process and time for data restoration, etc.

5.2 Logs and audit trails

The GxP standards in different countries and regions for electronic records and data management of drug or medical device development, production, operations, and use processes all focus on ensuring the authenticity, accuracy, integrity, and traceability of information throughout the lifecycle. With regard to traceability, relevant GxP standards prescribe that "Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming, or deleting data, including date and time." Customers in the healthcare industry should pay attention to the risk assessment results of the GxP system and enable the audit trail feature to ensure compliance with GxP requirements. Tencent Cloud provides a wide range of products and services for logs and audit trails. Customers can purchase and configure the selected products and services as needed. Tencent Cloud collects logs based on product features and customers' configurations. For more information, see “logs and audit trails”-relevant product introduction in Section 7.

According to Tencent Cloud's log management policy, the log feature needs to be enabled for Tencent Cloud products and supporting systems, including but not limited to system logs and application logs. The login activities and user operations related to backend Ops are monitored, and logs are generated through the security components, including but not limited to operation objects, operation time, operations, and status. The logs will be regularly uploaded to the remote server for storage and backup and cannot be deleted, modified, or replaced. On this basis, the Tencent Cloud security team collects the logs of each business and system on a regular basis to dig into and analyze the information on anomalies, identify system or operation anomalies, and implement full-chain log security audit.

5.3 Change and configuration management

According to the requirements set forth in GxP standards, all changes to computerized systems of customers in the healthcare industry, including system configurations, should be carried out in a controlled manner in strict compliance with the prescribed procedure. The procedure covers the evaluation, review, approval, change implementation, and verification processes and the records should be kept. Customers in the healthcare industry need to implement the change and configuration management processes for computerized systems or healthcare applications and ensure that all changes have been approved and are traceable.4

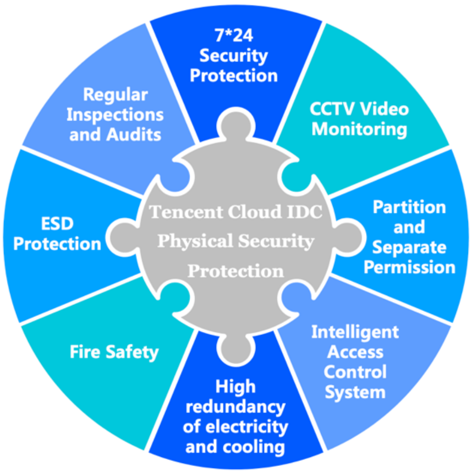
In order to provide better services for customers, Tencent Cloud maintains, upgrades, or optimizes the cloud platform, devices, systems, software, and other similar items on a regular or irregular basis. It has put in place a complete change management procedure to regulate and standardize the implementation of system changes and emergency system changes. Tencent Cloud requires that before any change is released, the change plan must include impact assessment and monitoring, rollback, and result verification, and be reviewed by relevant teams, including product, R&D, testing, security, and Ops. The change implementation team needs to assess the impact on the customers' business, keep the internal teams and customers well informed, and get approval for the change from the business owner. In the process of change implementation, the relevant personnel need to strictly comply with the requirements of the change process, keep a close watch after the release, and follow up on and verify the results. In addition, Tencent Cloud requires that all upgrades should be performed during off-peak hours to the extent possible, and grayscale release and verification be conducted in batches to minimize the impact on the production environment.

In addition to the process standardization, Tencent Cloud has built a dedicated change management platform to manage different types of changes. Tools are employed to ensure systematic implementation of the change management process, guarantee the quality of change release, and improve the efficiency of release implementation. The change management platform provides a range of services such as ticket creation, approval, notification, and release implementation and records the change application, approval, and implementation processes in detail, making the entire process traceable and auditable.

Tencent Cloud has established a reliable configuration management system. It centrally manages IT service components and configuration items through the configuration management database (CMDB), regulates the management of configuration items and the relationships amongst these items, and audits the CMDB on a regular basis to ensure the validity, accuracy, and integrity of the information of each configuration item. If configuration update is involved in the change process, the Ops personnel will update the version and information of the configuration item to the CMDB according to the change plan once the change is implemented.

5.4 Physical security

As a leading cloud service provider, Tencent Cloud is committed to providing secure, stable, continuous, and reliable physical infrastructure to meet the GxP requirements for physical security and ensure that the system is located in an appropriate place and armed with adequate physical security controls.


Tencent Cloud IDC Physical Security Protection
7*24 Security Protection
CCTV Video Monitoring
Partition and Separate Permission
Intelligent Access Control System
High redundancy of electricity and cooling
Fire Safety
ESD Protection
Regular Inspections and Audits

Physical security safeguards of Tencent Cloud IDC

(1) Physical access control

Tencent Cloud IDCs have established a comprehensive access control matrix according to the roles and permissions of personnel, and an access control system is deployed in each area of the IDC. Only authorized persons have access to the corresponding areas. Persons with temporary permissions should be accompanied by the IDC's onsite personnel or Ops personnel the whole time, and such permissions are only valid on the current day. IDC monitoring covers all critical areas and their entrances and exits, and 24/7 video surveillance and alarming systems without blind spots are deployed in critical areas to prevent unauthorized access.

(2) Physical environment security

According to the international standards and regulatory requirements for IDCs, Tencent Cloud has established a comprehensive IDC physical environment security management system. Tencent Cloud selects sites for, builds, or leases IDCs around the world in accordance with the international standards and local security requirements. All the IDCs are equipped with smoke alarming and fire protection systems. The power systems and air-conditioning systems are fully redundant systems with high stability, and any single point of failure will not affect the continuity of the power and cooling systems within the IDCs. Anti-static flooring is installed inside the IDCs, and all cabinets and wire slots use grounding wires to prevent any damage caused by static electricity to the equipment. Moreover, the onsite personnel inspect the IDC and equipment every day in strict compliance with the inspection checklist and plan. Once a security breach is detected, the emergency management process of the IDCs will be activated immediately.

(3) Internal and external audits

In addition to the above-mentioned physical protection measures, Tencent Cloud IDCs conduct strict internal and external audits and compliance checks on the data center environment, physical security management, etc. Inspection reports are developed accordingly. The identified issues are fixed in a timely manner, and continuous improvements are made to ensure the physical and environmental security of Tencent Cloud IDCs.

5.5 Network security

According to Article 20 of the Requirements for Drug Records and Data Management (Trial), organizations that adopt computerized systems for electronic records should ensure the security and stability of the network environment hosting their systems. For on-cloud GxP systems, customers in the healthcare industry need to take measures such as access control or communication encryption to ensure the security and reliability of information transfer and data sharing over the virtual network. Tencent Cloud has developed and implemented multi-level network security governance architecture and policies to improve the robustness of the underlying network of its platform, including:

1) Network isolation

Tencent Cloud boasts a full-fledged network security architecture and sets up network perimeter firewalls to protect the internal network from unauthorized access. The internal network follows a strict isolation policy. The internal network is divided into various network zones such as the office network, isolation zone network, and operating network, etc., with well-defined access control and perimeter protection between the zones. In particular, access to the production environment requires login through the jump server, and unauthorized Tencent Cloud employees are not allowed to log in to the jump server. With regard to network isolation for cloud customers, Tencent Cloud uses web console access control, Tencent Cloud API authentication, and other measures to ensure that the customers can only access their own cloud resources. Additionally, Tencent Cloud offers virtual private clouds (VPCs) that allow customers to implement complete logical isolation by configuring the network environment, route table, and security policies.

2） Network configuration security

Tencent Cloud has set network security baseline standards for the security configuration of network devices. For example, security settings on network devices must be enabled, only necessary network service features and protocols are opened, wireless networks of any form are prohibited from connecting to the production networks, and the security policies of virtual networks should be aligned with those of physical networks. The configuration items of network devices are automatically scanned through the configuration scanning tool. In case of any anomalies, alarm will be triggered immediately, and a ticket will be created automatically.

3） Network communication security

Tencent Cloud requires web services open to the public network to configure the HTTPS transfer protocol and adopt secure transfer protocols to ensure the security of data transferred over the public network. For communications between the customer/its third-party partners/subcontractors and Tencent Cloud, customer needs to take encryption measures or use encryption channels based on its own security requirements and actual monitoring capabilities to ensure the confidentiality and integrity of data in the transfer process.

4） Network attack protection

Tencent Cloud implements multi-point network security monitoring and multi-layer protection through the internal network attack protection center. Through traffic analysis, the center detects various types of network attacks in real time and quickly sends alarms against the network attacks to help Tencent Cloud businesses resist network attacks (such as DDoS attacks), creating a secure, stable, and sound network environment for businesses.

5.6 Server security

According to the GxP standards, when using computerized systems to process and store electronic records of GxP activities, the healthcare industry should ensure that the server can sustain the normal system operations without negatively affecting GxP-regulated businesses. Therefore, customers need to develop a security protection system for cloud servers. Tencent Cloud provides best practices guidelines for security hardening of cloud servers and a range of cloud products that can enhance server security capabilities. Customers can choose the suitable solutions or products as needed to mitigate network security risks such as data breaches.

In terms of server security, Tencent Cloud takes a variety of protection and hardening measures to improve the underlying server security.

(1) Intrusion detection and protection

Intrusion refers to the malicious behavior in which hackers bypass access control by taking advantage of website and server vulnerabilities, stealing accounts, or launching brute force attacks to illegally obtain server permissions, which can cause enormous losses to businesses. Tencent Cloud requires that server security protection and intrusion detection software must be deployed on business servers, and the software installation rate be monitored in real time. Tencent Cloud adopts an intrusion detection model featuring distributed data sampling and centralized analysis and protection. The detection system analyzes and mines data based on the feature code and user behaviors, matches them with intrusion rules, and then sends alarms and provides protection accordingly.

(2) Operating system security

Tencent Cloud has set and implemented infrastructure and virtualization security management standards. It conducts security baseline checks on the server's operating system and draws up system hardening plans based on the information security assessment results, including disabling infrequently used or unnecessary services and programs in the system and using strong passwords. As required by Tencent Cloud, the Windows system must be installed with antivirus software, configured with automatic virus database updates, and checked for security every month, and the updates and patches must be installed to the operating system in a timely manner. Further, patch installation needs to follow the change management process, and a comprehensive test on the hardened system should be conducted to ensure that system hardening will not negatively affect businesses.

5.7 Application security

According to the GxP standards, applications of the computerized systems used by the regulated organizations should comply with the applicable legal requirements and management requirements. Customers in the healthcare industry need to ensure that their applications meet business needs and compliance requirements. Tencent Cloud guarantees the security and reliability of its products and services through the closed loop of application protection, vulnerability detection and fix.

(1) Application protection

Leveraging its mature security capabilities, Tencent Cloud has developed a multi-level, all-round security protection system for its cloud applications. Resources open to the public network should be connected to security protection systems such as vulnerability scanning, DDoS protection, and application firewalls. In terms of web protection capabilities, Tencent Cloud withstands attacks through multi-dimensional defense strategies such as web intrusion prevention, zero-day vulnerability fix, bot management, and DNS hijacking detection, ensuring the secure operations of systems and services in the cloud.

(2) Application vulnerability detection

Tencent Cloud adopts multiple detection methods such as high-risk service/port detection, management backend openness detection, server intrusion detection, and container operations detection. In addition, Tencent Cloud also scans platforms and products for vulnerabilities on a regular basis. With regard to vulnerability scanning, Tencent Cloud requires that a vulnerability prevention and protection system must be deployed on external web systems, to scan Tencent Cloud's web service servers through "scheduled tasks", so as to quickly identify and address risks in businesses and prevent web vulnerabilities from being maliciously used. Tencent Cloud conducts penetration testing on critical systems, where external and internal attacks are stimulated, and the threats and vulnerabilities that Tencent Cloud has previously encountered are taken into account when the attack vector is set. Tencent Cloud carries out red vs blue team exercises to verify the overall level of security protection, identify risk blind spots, and improve the response efficiency. Through such exercises, the entire security protection system has been continuously improved.

(3) Vulnerability fix

The Tencent Cloud security vulnerability management platform automatically creates tickets for the security vulnerabilities or risks discovered. The corresponding product department needs to perform timely vulnerability assessments and take actions based on the type and risk level of the security ticket. It also needs to determine the rectification measures and fix plan based on root cause analysis. If the vulnerabilities discovered in the assessment may affect customers, Tencent Cloud will keep them informed of the vulnerability overview, impact, and other information through official announcements on the website and internal messages, and provide fix suggestions and detailed directions for them.

5.8 Identity authentication and access control

According to the GxP standards, healthcare organizations adopting computerized systems for their business processes should ensure that only authorized persons can use the system or access the data in the system. Customers in the healthcare industry should be responsible for identity authentication and permissions management within their organization to prevent unauthorized access to the systems or data. As a leading cloud service provider, Tencent Cloud has launched Cloud Access Management (CAM) to help customers effectively manage their accounts and subaccounts with Tencent Cloud. With CAM, customers can securely manage the access permissions, resources, and use permissions of their Tencent Cloud account. For more information on the CAM, see Section 7.

As to the daily operations and maintenance of the underlying infrastructure and backend, Tencent Cloud has adopted strict cloud platform operations and maintenance security management policies to regulate its employees' access to and operations on CVM (Cloud Virtual Machines) instances to reduce the risk of unauthorized access to information assets. Tencent Cloud also ensures that its internal access permissions matrix complies with the principles of least privilege and segregation of duties. These policies include the following:

- The accounts of all users within Tencent Cloud must have a unique ID to ensure that the account uniquely corresponds to the operator.
- Tencent Cloud's new hires are assigned minimum permissions required by their role. Ops management staff are only authorized when necessary. They can log in to the jump server and the target server through two-factor authentication to perform Ops operations.
- The Tencent Cloud security team deploys security components to record operations on the jump server and the server. Login activities and user-sensitive operations such as modifying, deleting, or transferring files are all monitored through the security components.

5.9 Incident response

In recent years, the healthcare systems around the world have suffered network attacks from time to time, and the healthcare industry has become a common target of attacks. The GxP standards of various countries also require regulated healthcare organizations to establish operating procedures for security incidents such as system failures and data errors to ensure that all incidents are properly recorded, assessed, and handled, and preventive and corrective actions are taken based on root cause analysis. For security incidents within the scope of Tencent Cloud's responsibility, Tencent Cloud has developed a standardized and streamlining emergency response mechanism to promptly respond to the security incidents, notify the customers, and help them deal with the incidents. For security incidents within the scope of the customers' responsibility, Tencent Cloud will also provide necessary support for them to address the incidents.

According to Tencent Cloud's security incident emergency response mechanism, once a security alarm is triggered, the cloud security team will evaluate and rate the risk of the incident according to the degree of impact and urgence. The relevant team will initiate the emergency response plan to prevent the incident from evolving, investigate it through logs and other methods, identify the attack path, causes of alarms, and impact, and then take actions such as troubleshooting to restore the systems or services. A business continuity management plan will be implemented if necessary. Once the incident is eliminated, the department concerned should conduct a review and root cause analysis to take corrective measures and further improve the existing security policies. Tencent Cloud will inform the parties concerned of the incident response and handling processes according to the applicable laws, regulations, and requirements.

In coordination with the customers' incident response procedure, Tencent Cloud provides 24/7 technical support with comprehensive operations security capabilities to help its customers meet compliance requirements. Tencent Cloud offers multiple channels to deal with customers' problems and feedback, including 24/7 tickets, 24/7 hotline, smart customer service, and self-service. Tencent Cloud's customer service team and technical experts provide rapid and effective support to help customers efficiently identify the root cause of problems, keep track of the incidents, and find suitable solutions to various issues with Tencent Cloud product features, infrastructure, underlying network, and servers. If the customer is an organization with complex business systems, it can also choose other applicable service packages to get tailored support through dedicated support groups, technical support managers, value-added services, etc.

5.10 Business continuity management

According to the GxP requirements, healthcare organizations should develop contingency plans for computerized systems that support critical business processes based on risk assessment results, and ensure business continuity in the event of a failure. In order for continuous and stable operations of the healthcare system, the integrity of patient data, and user safety, customers in the healthcare industry need to draw up business continuity plans in light of the sensitivity of business scenarios and ensure the robustness of their healthcare system components. Tencent Cloud guarantees the business continuity of its cloud platforms and services by virtue of high architecture availability, disaster tolerance of networks and computing units, and daily business continuity management.

(1) High architecture availability

Tencent Cloud operates 70 availability zones in 26 regions around the world, with over ten ISPs (Internet Service Provider) at the underlying layer. Based on the business development needs, customers can choose to flexibly deploy their businesses in different regions for the purpose of disaster recovery. In addition, the architecture and environment of Tencent Cloud IDCs lend themselves to redundancy and disaster recovery, including the power supply system, air-conditioning system, fire detection and protection system, ensuring the high availability of customers' underlying infrastructure.

(2) Disaster tolerance of networks and computing units

Tencent Cloud networks use N*N redundancy in construction and allow for traffic scheduling based on route path priority and route reachability to ensure that network services will not be interrupted due to single point of failure. Tencent Cloud has the basic network disaster recovery plans in place. In the event of IDC interconnection failures, the traffic will be switched from the failed nodes to the normal ones, to enhance the cross-region disaster recovery capabilities of Tencent Cloud networks. In response to public network failures on the part of ISPs, Tencent Cloud IDC network egresses are connected to multiple ISPs across various regions, which can effectively reduce the ongoing impact. Tencent Cloud computing units also adopt N*N redundancy, that is, a single failing computing unit will be eliminated in real time through the scheduler to ensure service availability.

(3) Daily business continuity management

Tencent Cloud attaches great importance to the business continuity management of its cloud platforms. Internal processes are implemented to ensure that business operations can meet the availability requirements and support customers in integrating their business continuity plans. Additionally, Tencent Cloud is one of the first batch of cloud service providers in China to have an ISO 22301 compliant business continuity management system.

Tencent Cloud product teams have established business continuity management plans and contingency plans based on the results of analysis of business impact on systems and business processes, so that Tencent Cloud can recover and continue to operate the businesses and systems as required in the event of business interruptions. Tencent Cloud regularly carries out drills of the continuity plans and contingency plans, assess the rationality and effectiveness of the plans based on the results of the drills, and review and adjust as appropriate the recovery time objective, recovery point objective, operating procedure, or job responsibilities. Tencent Cloud works with partner IDC ISPs to regularly design various disaster and emergency scenarios, develop contingency plans, and carry out emergency response drills to ensure that the personnel can complete the business restoration process methodically.

6. Electronic Records and Data Management

6.1 Procedure for electronic records and data management

According to the Requirements for Drug Records and Data Management (Trial), healthcare organizations engaged in drug development, production, distribution, and use processes shall abide by the applicable laws, regulations, rules, standards, and norms, establish operating procedures and management systems, and specify the requirements for records and data management. As such, healthcare organizations should establish a data security management system based on their actual situation. Tencent Cloud has established data security systems and management specifications to clarify the data security processes and standards that Tencent Cloud employees should follow, including data classification and grading, lifecycle management, security risk assessment, security audit, and security incident handling. The goal is to increase Tencent Cloud's overall level of data security and reduce the risk of data breach.

6.2 Protection of electronic records and data

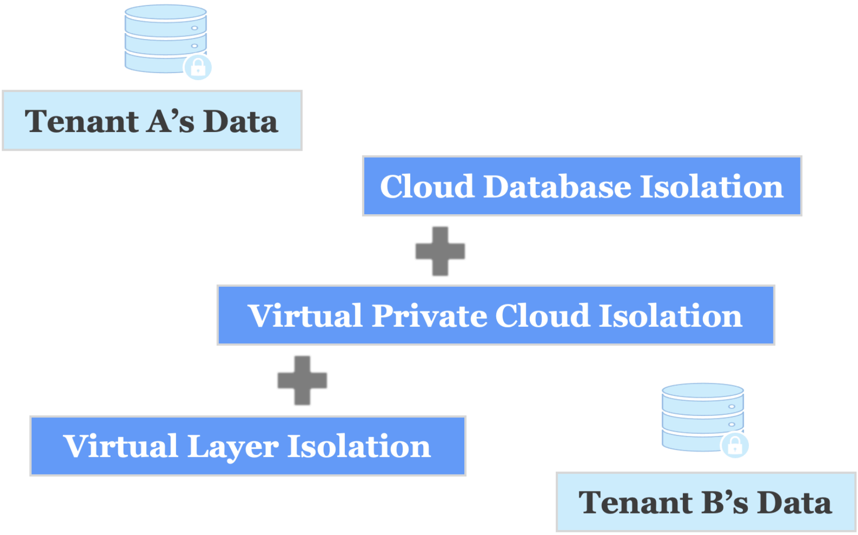
As the integrity and accuracy of health data have a direct impact on patients' health and safety, data is considered as the lifeblood of the healthcare industry. According to Articles 4, 5, and 8 of the Requirements for Drug Records and Data Management (Trial) and Sections 11.10(b), 11.10(c), and 11.30 of Title 21 of the Code of Federal Regulations Part 11 "Electronic Records; Electronic Signatures – Application and Scope" (21 CFR Part 11), healthcare organizations using computerized systems to create, modify, maintain, or transfer electronic records should adopt appropriate procedures and controls to ensure the authenticity, integrity, and confidentiality of electronic records from creation to destruction, so that they can accurately and conveniently retrieve, inspect, or replicate the records during the retention period.

Customers in the healthcare industry have full control over their business data in on-cloud GxP systems and are ultimately responsible for security management of their business data stored in the cloud. Therefore, they need to implement appropriate administrative measures or use data security products or features in Tencent Cloud based on their business needs and the GxP requirements to ensure the authenticity, accuracy, integrity, and traceability of data in collection, processing, storage, and other activities.

The Tencent Cloud platform comes with multiple administrative measures and technical means to help customers ensure the confidentiality, integrity, and availability of their data in the cloud.

(1) Data confidentiality:

- **Data isolation:** Tencent Cloud uses multi-layer technical isolation methods to ensure that in the same resource pool, a customer's data is invisible to other customers. This technically guarantees that a customer cannot access, get, or tamper with other customers' data.
    - **Virtual layer:** Tencent Cloud employs mature hardware virtualization technologies to provide complete inter-tenant virtual resource isolation capabilities for cloud servers and other resources at the virtual layer. Logical access controls prevent interconnection and mutual access between the networks, memories, disks, and other resources of different users to guarantee that each customer can only access the cloud computing resources they have purchased. As such, data isolation between different customers can be achieved.
    - **Network layer:** Virtual Private Cloud (VPC) is a dedicated cloud network space built by Tencent Cloud for its customers. Customers can configure the VPC to logically isolate their network from others'. They can customize IP ranges, IP addresses, and routing policies and create network ACLs and security groups to filter traffic at subnet and server levels. This enables data isolation between customers through complete network isolation.
    - **TencentDB layer:** When Customers use TencentDB instances, Tencent Cloud adopts an whitelist filtering mechanism to isolate the network layer by configuring firewall policies. Through the permission management mechanism for database instances, Tencent Cloud ensures that each customer can only access its own data but not the data of other customers. In addition, Tencent Cloud offers dedicated cluster databases which give customers exclusive access to the physical cluster resources and enable them to flexibly create database instances with custom specifications.



Data isolation between Tencent Cloud tenants

- **Data encryption:** Tencent Cloud provides encryption features for customer data in transfer and in storage and allows customers to manage their own encryption keys. For data in transfer, Tencent Cloud encrypts the transmission between the customer and Tencent Cloud console over the internet with HTTPS. The transmission between customers and Tencent Cloud through TencentCloud API also supports HTTPS encryption in order to guarantee the data confidentiality. For data in storage, Tencent Cloud provides encryption key management services and a variety of products for data storage encryption. Customers can purchase and configure the products as needed to protect their static data.
- **Data destruction:** Tencent Cloud pays high attention to the confidentiality of data when it is destructed. For business data stored in the cloud by customers in the healthcare industry, when the cloud service agreement is terminated or customers delete the data, Tencent Cloud will use an industry recognized mechanism to erase and overwrite the data in the storage medium as agreed upon with customers to ensure that the data stored in the data disk is completely erased and that the data cannot be restored after deletion. As to the destruction of damaged or retired storage media, Tencent Cloud has developed a comprehensive process and solution to handle the destruction of storage medium containing sensitive data through degaussing, physical destruction, etc. It ensures that the entire process is a controllable closed loop, and records and videos are traceable.

(2) Data integrity:

- **Data integrity verification:** Tencent Cloud adopts the multi-replica redundancy and erasure code technology for data storage. Once integrity errors are detected, restoration measures will be taken immediately to improve data fault tolerance. When customers send requests through TencentCloud API, each request should include signature information in the public request parameters to verify customer's identity and ensure the integrity of the request.
- **Data access control:** As a cloud service provider, Tencent Cloud guarantees that it will not access or use customers' business data unless otherwise stipulated by laws and regulations or agreed by both parties. Tencent Cloud implements strict operation and maintenance access control procedures and technical measures to prevent the operation and maintenance personnel from performing unauthorized operations or invalid modifications on the data stored in the cloud.

(3) Data availability:

- **Support for multiple copies:** Tencent Cloud provides multiple copies and backup services, and customers can choose the backup services based on their business needs. Tencent Cloud allows customers to store data on different storage nodes to prevent data loss due to hardware failure or other factors.
- **Disaster recovery capabilities:** Tencent Cloud operates 70 availability zones in 26 regions around the world. Availability zones (AZs) refer to Tencent Cloud's physical IDCs that are in the same region and have independent power and network resources. They are designed to ensure that failures within one AZ can be isolated without affecting other zones. A variety of Tencent Cloud's basic products, such as Cloud Virtual Machine (CVM) and TencentDB, have disaster recovery capabilities within one cluster and across AZs to help customers promptly restore the applications and data in the event of a disaster. This shortens business interruptions and ensures high availability of data.

For more information on data security, see **Tencent Cloud Data Security White Paper**.

7. How Tencent Cloud products and services support GxP compliance

Apart from helping customers in the healthcare industry ensure GxP compliance through its cloud platform management processes and technical measures, Tencent Cloud offers a full range of diverse products and tools to support customers in building a secure and stable GxP system in the cloud. The following are some selected Tencent Cloud products or services and describes how customers can use them to ensure the security and compliance of their GxP systems in the cloud.

For more information, see Tencent Cloud **Products & Services**.

Domain	Product/Service	Feature
System development lifecycle	CODING DevOps	CODING DevOps consists of multiple products and services such as Code Repositories, Project Management, Test Management, Continuous Integration, and Artifact Repositories, which provide all needed for software development from conception to delivery, enable R&D personnel to collaborate efficiently in the cloud and practice agile development and DevOps, and increase the quality and speed of software delivery.
	WeTest	WeTest consists of multiple products such as standard compatibility testing, expert compatibility testing, mobile game security testing, and remote debugging, serving a high number of Tencent's games. It boasts an all-round security protection system encompassing compatibility testing, stress testing, performance testing, security testing, and remote debugging and other directions to comprehensively protect customer’s information security.
Data migration and verification	Data Transmission Service (DTS)	DTS enables customers to migrate their databases to Tencent Cloud with no business interruptions, create a high-availability database architecture through real-time sync channels, and use data subscription to meet their requirements

Domain	Product/Service	Feature
		for commercial data mining and business asynchronous decoupling, etc.
	Migration Service Platform (MSP)	MSP integrates various migration tools and provides unified monitoring. Customers can choose Tencent Cloud's own migration tools or officially certified third-party migration tools. MSP enables customers to migrate their systems to the cloud conveniently and efficiently and stay up to date with the migration progress. It allows customers to centrally monitor the migration process to prevent potential damage to the integrity of data.
Data backup and restoration	Cloud Object Storage (COS)	COS is a distributed storage service launched by Tencent Cloud. It has no directory hierarchy or data format restrictions, can accommodate massive amounts of data, and supports access over the HTTP/HTTPS protocol. Data stored in COS can be stored in multiple specified regions at the same time through the cross-region replication feature, which ensures that the complete data can still be found and recovered through data redundancy in case of accidental loss of some data. Plus, as multiple copies of data are stored in different regions, the loss of data in one single region due to irreversible disasters can be avoided, thus achieving the effect of multi-redundancy backup and remote disaster recovery, guaranteeing the data durability and stability, and protecting important data with multiple security mechanisms.
	Cloud Block Storage (CBS)	CBS provides a persistent block storage service for CVM. It boasts 99.9999999% reliability. Before each storage write request is returned to user, CBS ensures that the data has been successfully written into three replicas and stored across racks. The backend replication mechanism guarantees that

Domain	Product/Service	Feature
		data migration and restoration can be quickly implemented once a replica is in failure, preventing customers' applications from any threat in the advent of component faults.
	Cloud File Storage (CFS)	CFS provides a secure, reliable, and scalable shared file storage service. Each file stored in a CFS standard file system has three redundant copies in an AZ. CFS features an extremely high availability and reliability and supports restricting permissions on the client through user isolation, network isolation, and access whitelists.
Logs and audit trails	CloudAudit	CloudAudit enables customers to perform supervision, compliance checks, operational reviews, and risk reviews for their Tencent Cloud account. With CloudAudit, customers can record, continuously monitor, and retain the account activities related to operations in the Tencent Cloud infrastructure. It provides the history of customers' Tencent Cloud account activities, including operations performed through Tencent Cloud console, APIs, command line tools, and other Tencent Cloud services, which simplifies security analysis, resource change tracking, and troubleshooting.
	Cloud Log Service (CLS)	CLS is a one-stop log service platform that provides a wide variety of log services such as log collection, storage, search, chart analysis, and shipping. It assists customers in implementing business Ops, service monitoring, log auditing, and more.
Network Security	Virtual Private Cloud (VPC)	VPC is a dedicated cloud network space built by Tencent Cloud. It provides network services for customers' resources in Tencent Cloud, with complete logical isolation between VPCs. Customers can manage their VPC

Domain	Product/Service	Feature
		through software-defined networks, including the configuration of IP addresses, subnets, route tables, network ACLs, flow logs, and other features. VPC supports internet connections through multiple methods, such as EIP and NAT Gateway. Customers can connect their on-premises IDC to Tencent Cloud through VPN Connections to flexibly build a hybrid cloud.
	VPN Connections	VPN Connections quickly creates a secure, reliable, and encrypted tunnel on the internet based on tunneling technology to implement interconnection transfer services between IDCs and resources in Tencent Cloud. It features simple configuration, immediate effect of cloud configuration, high reliability, and a gateway availability of 99.95%, ensuring stable and continuous business connections. It helps customers easily implement remote disaster recovery, hybrid cloud deployment, and other complicated business scenarios.
	Anti-DDoS	Anti-DDoS provides comprehensive, efficient, and professional DDoS protection capabilities in forms of multiple Anti-DDoS solutions such as Anti-DDoS Pro and Anti-DDoS Advanced for enterprises and organizations to combat DDoS attacks. It leverages its abundant and premium DDoS protection resources and the ever-evolving "proprietary + AI recognition" cleansing algorithm to guarantee the stable and secure operations of customers' business.
	Cloud Firewall (CFW)	Cloud Firewall (CFW) is an SaaS firewall based on the public cloud environment. It provides network edge protection, and addresses security and management needs for centralized access control and log audit. In addition to the features of

Domain	Product/Service	Feature
		traditional firewalls, CFW supports multi-tenancy and elastic scaling and is an essential network security infrastructure for cloud migration..
Server security	Cloud Workload Protection (CWP)	Based on Tencent Security's massive amounts of threat data, CWP leverages machine learning to provide a wide variety of security protection services, including asset management, trojan detection and prevention, intrusion detection, vulnerability alerting, and security baseline. It helps build a security protection system to cope with major network security risks faced by servers. It supports unified security protection for non-Tencent Cloud servers and enables effortless security intelligence sharing in Tencent Cloud, providing the same level of protection for private IDCs as in the cloud.
Application security	Web Application Firewall (WAF)	WAF helps users in and outside Tencent Cloud easily cope with various types of website and web service security issues, such as web attacks, intrusions, vulnerability exploits, trojans, tampering, backdoors, and crawlers. It enables customers to transfer the pressure on defense against web attacks to WAF clusters and get Tencent Cloud's security protection capabilities in seconds, guaranteeing the secure operations of protected websites and web services.
	Vulnerability Scan Service (VSS)	Built on Tencent's 20 years of experience in security operations, VSS automatically checks customers' network assets, including devices and applications, and identifies the risks. Specifically, it enables regular security scans, continuous risk alarming, and vulnerability detection in terms of availability, security, and compliance and offers professional advice on fix and repair to help lower customers' security risks.

Domain	Product/Service	Feature
Identity management and access control	Cloud Access Management (CAM)	CAM is a web-based Tencent Cloud service that helps customers securely manage and control the access permissions, resources, and use permissions of their Tencent Cloud account. With CAM, customers can create, manage, and terminate users (groups), and control the Tencent Cloud resources that can be used by the specified user through identity and policy management.
Incident response	Cloud Monitor (CM)	CM allows customers to configure threshold alarms for Tencent Cloud product resources and custom resources. It has multiple features such as comprehensive cloud product data monitoring, smart data analysis, real-time exception alarms, and visual data display. It helps customers stay up to date with the health status of services and cloud products, improving the operations and maintenance efficiency while reducing the costs thereof.
Electronic records and data protection	Data Security Center (DSGC)	DSGC automatically organizes customers' cloud data assets and performs classification, grading, and security risk assessment of customers' data. It works with various security capabilities of Tencent Cloud to form a closed network of data security protection and help customers maximize the security benefits.
	Key Management Service (KMS)	KMS is a security management solution that enables customers to easily create and manage keys and protect their confidentiality, integrity, and availability, helping meet customers' key management and compliance needs in multi-application and multi-business scenarios.

Conclusion

Driven by the industry trend of digital transformation, a growing number of healthcare organizations are migrating their business systems and data to the cloud. When building GxP systems based on the infrastructure or cloud services provided by cloud service providers, customers should adequately plan and evaluate cloud migration. For one thing, customers need to get a grasp of the cloud architecture of their GxP systems. For another, they need to assess whether the cloud service provider has sufficient security capabilities and controls to ensure system stability and data security.

With a focus on quality management, operations and maintenance, and electronic records and data management, this white paper describes how Tencent Cloud ensures the quality, security, and reliability of its products and services through its internal management processes and security technologies to help customers within the healthcare sector achieve compliance with GxP standards. Based on years of cloud service experience and security capabilities, Tencent Cloud offers a full range of products and services in alignment with industry best practices. Leveraging its professional security capabilities and technologies, Tencent Cloud provides continuous security protection for customers' GxP systems in the cloud and delivers fast security incident response. It empowers its customers to build a robust security protection system for GxP systems and further strengthen their GxP compliance management capabilities, safeguarding their journey to the cloud every step of the way.

Appendix: GxP Standards and Mapping Table

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
1	Risk management	Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity, and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.	Customers should carry out risk assessments throughout the lifecycle of their GxP systems. Tencent Cloud embeds risk management into the entire lifecycle of the systems. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation".
2	Personnel	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons, and IT. All personnel should have appropriate qualifications, level of access, and defined responsibilities to carry out their assigned duties.	Customers should ensure that the personnel involved with GxP systems have the necessary system and procedure operation skills and qualifications. Tencent Cloud has established and implemented personnel training mechanisms to ensure that its personnel have the required qualifications, abilities, and awareness of information security. For more information, see Section 4.4 "Personnel management".
3	Supplier management	3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify, or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these	Customers are obligated to evaluate supplier qualifications and sign agreements with the suppliers to clearly define the responsibilities of both parties.

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		agreements should include clear statements of the responsibilities of the third party. IT departments should be considered analogous. 3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. 3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	As a cloud service provider, Tencent Cloud will take into account customers' GxP compliance requirements, assist customers with on the supplier evaluation and matters pertaining to agreements. For more information, see Section 4.5 "Supplier management". Tencent Cloud has established and implemented procedures to evaluate its quality management system on a regular basis. The goal is to ensure that the quality management system is aligned with its quality policy and objectives and meets customers' demand for GxP compliance. For more information, see Section 4.2 "Quality management audit".
4	Validation	4.1 The validation documentation and reports should cover the relevant steps of the lifecycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures, and records based on their risk assessment. 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. 4.3 An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems, an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	Customers should determine the scope and degree of validation based on the risk assessment results to ensure that the system components perform as intended. Tencent Cloud implements product and service quality and security management throughout the system development lifecycle and ensures that all relevant components remain in a valid state. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation". Tencent Cloud has established a complete change management procedure, specification, and operations for standard and emergency system changes. For more information, see Section 5.3 "Change and configuration management".

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		4.4 User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the whole lifecycle. 4.5 The regulated user should take all reasonable steps to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. 4.6 For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the lifecycle stages of the system. 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	
5	Data	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	GxP-regulated healthcare organizations should use appropriate built-in checks or encryption methods based on the business processes to ensure that electronic data is exchanged and processed in a secure manner. Tencent Cloud encrypts the communication between customers and the Tencent Cloud console over the internet with HTTPS. The communication between customers and

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			Tencent Cloud through TencentCloud API also supports HTTPS encryption. For more information, see Section 6.2 "Protection of electronic records and data".
6	Accuracy checks	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should take measures to ensure the accuracy of manually entered data.
7	Data storage	7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability, and accuracy. Access to data should be ensured throughout the retention period. 7.2 Regular backups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Customers have full control over their business data in on-cloud GxP systems and are ultimately responsible for security management of their business data. Customers need to implement appropriate administrative measures or use data security products or features in Tencent Cloud to ensure the authenticity, accuracy, integrity, and traceability of data in collection, processing, storage, and other activities. The Tencent Cloud platform comes with multiple administrative measures and technical means to help customers ensure the confidentiality, integrity, and availability of data in the cloud. As for Tencent Cloud's data backup services, customers can submit a ticket to get additional information on backup and validation. For more

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			information, see Sections 6.2 "Protection of electronic records and data" and 5.1 "Data backup and restoration".
8	Printouts	8.1 It should be possible to obtain clear printed copies of electronically stored data. 8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	This requirement does not apply to Tencent Cloud. Customers have full control over their data stored in the cloud.
9	Audit trails	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Customers should ensure that the system retains logs for the purpose of audit trails. Tencent Cloud has established log and audit management systems. It records the logs of backend operations and carries out audits periodically. For more information, see Section 5.2 "Logs and audit trails".
10	Change and configuration management	Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Customers should ensure that control processes and operation specifications are in place for any changes to their GxP systems. Tencent Cloud has established strict change and configuration management processes for its products and supporting platforms. It ensures that the changes are secure and controllable through the change management platform.

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			For more information, see Section 5.3 "Change and configuration management".
11	Periodic evaluation	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Customers should conduct periodical assessments of their computerized systems to verify their GxP compliance. For the GxP components provided by Tencent Cloud, system quality and security are audited every year by an independent third-party organisation to ensure that Tencent Cloud products or services remain in a valid state. For more information, see Section 4.2 "Quality management audit".
12	Security	12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. 12.2 The extent of security controls depends on the criticality of the computerized system. 12.3 Creation, change, and cancellation of access authorizations should be recorded. 12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming, or deleting data, including date and time.	As for physical controls, Tencent Cloud is responsible for the underlying physical security of GxP systems based on Tencent Cloud. Tencent Cloud ensures that physical controls are in place through access control, physical environment management, periodical inspections and audits, etc. For more information, see Section 5.4 "Physical security". With regard to logical controls, customers should take identity authentication and access control measures within the organization to ensure that internal personnel's access to their GxP business systems is under control. Tencent Cloud adopts various identity verification and access control

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			measures to ensure that backend Ops is authorized, and logs are kept for security audits. For more information, see Section 5.8 "Identity authentication and access control".
13	Incident management	All events, not only system failures and data errors, should be reported and assessed. The root cause of a critical event should be identified and should form the basis of corrective and preventive actions.	Customers should establish an incident management process and take appropriate corrective and preventive actions. Tencent Cloud has established a complete incident response process to ensure that events are dealt with promptly to mitigatenegative impact. If an incident may affect the customers' businesses, Tencent Cloud will inform the customers as soon as possible and provide suggestions on incident handling. For more information, see Section 5.9 "Incident response".
14	Electronic signature	Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the scope of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations using electronic signatures should comply with the applicable regulations.
15	Batch release	When a computerized system is used for recording certification and batch release, the system should allow only qualified persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable regulations on batch release.

Annex 11 "Computerized Systems" to EudraLex Volume 4 GMP by the European Medicines Agency			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
16	Business continuity	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and should be appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Customers should develop business continuity plans and carry out exercises for GxP systems on the basis of business impact analysis to ensure the effectiveness. Tencent Cloud has established a business continuity management system and developed contingency plans for its products and services. It will also coordinate with customers on their business continuity plans. For more information, see Section 5.10 "Business continuity management".
17	Archiving	Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Tencent Cloud adopts various data protection measures to assist customers in ensuring the accessibility, readability, and integrity of the archived data in Tencent Cloud. For more information, see Section 6 "Electronic Records and Data Management".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 3	Risk management	Risk management should be applied throughout the lifecycle of the computerized system, taking into account patient safety, data integrity, and product quality. As part of quality risk management, the extent of validation and data integrity controls should be based on written risk assessment results.	Customers should carry out risk assessments throughout the lifecycle of their GxP systems. Tencent Cloud embeds risk management into the entire lifecycle of systems. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation".
Article 4	Supplier management	Organizations should establish operating procedures for the management of computerized system vendors. They should sign a formal agreement with the vendor of products or services (such as installation, configuration, integration, verification, maintenance, and data processing) to clarify the responsibilities of both parties. Organizations should provide documentation concerning supplier quality systems and audit information based on risk assessment results.	Customers are obligated to evaluate supplier qualifications and sign agreements with the suppliers to clearly define the responsibilities of both parties. As a cloud vendor, Tencent Cloud will coordinate with customers' GxP compliance requirements and their work on supplier evaluation and matters pertaining to agreements. Tencent Cloud will also present its ISO 9001 certification to customers upon request. For more information, see Section 4.5 "Supplier management".
Article 5	Personnel	Close collaboration between relevant functions is required in various activities throughout the lifecycle of computerized systems, such as verification, use, maintenance, and management. The responsibilities and permissions of the personnel who use and manage the computerized systems should be clearly defined, and the personnel should receive training on the use and management of such systems. Experts	Customers should ensure that the personnel involved with GxP systems have the necessary system and procedure operation skills and qualifications. Tencent Cloud has established and implemented personnel training mechanisms to ensure that its personnel have the required qualifications, abilities, and awareness of

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		should be available to provide training and guidance on the design, verification, installation, and operations of computerized systems.	information security. For more information, see Section 4.4 "Personnel management".
Articles 6–9	Validation	Article 6 Computerized system validation includes application and infrastructure validation, of which the scope and degree should be based on scientific risk assessments. The scope and purpose of computerized systems should be taken into full account in risk assessments. A computerized system should remain in a valid state throughout its lifecycle. Article 7 Organizations should establish a list of all computerized systems involved in the quality management process of pharmaceutical products, indicating the functions related to pharmaceutical quality management. The list should be updated in a timely manner. Article 8 Organizations should assign dedicated persons to review general-purpose commercial software and ensure that it meets the needs of users. Organizations should establish appropriate operating procedures for the validation of custom computerized systems to evaluate their quality and performance throughout their lifecycle. Article 9 In case of data conversion or migration, it should be confirmed that the value and meaning of the data have not changed.	Customers should determine the scope and degree of validation based on the risk assessment results and validate the applications and architecture to ensure that the system functions as intended. Tencent Cloud implements product and service quality and security management throughout the system development lifecycle and ensures that all relevant components remain in a valid state. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation". Tencent Cloud has established a complete change management procedure, specification, and operations for standard and emergency system changes. For more information, see Section 5.3 "Change and configuration management".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 10	System	Systems should be installed at suitable locations to prevent any disturbances from external environmental factors.	As for physical controls, Tencent Cloud is responsible for the underlying physical security of GxP systems based on Tencent Cloud. Tencent Cloud ensures that physical controls are in place through access control, physical environment management, periodical inspections and audits, etc. For more information, see Section 5.4 "Physical security".
Article 11	System	Critical systems should have detailed documentation (with drawings when necessary), which should be updated in a timely manner. The documentation should describe in detail how the system works, its purpose, safeguards and scope of application, the main characteristics of the operation mode, and how it connects with other systems and programs.	Customers should create documentation concerning GxP systems. The documentation and API/SDK call methods for Tencent Cloud services or products can be found on the Tencent Cloud **Products & Services** page.
Article 12	System	Software is an essential component of every computerized system. Based on the risk assessment results, organizations should implement hierarchical management on the software they use (such as software vendor audit) and evaluate the supplier quality assurance system, so as to ensure that the software meets their needs.	Customers are obligated to evaluate supplier qualifications and sign agreements with suppliers to clearly define the responsibilities of both parties. As a cloud service provider, Tencent Cloud will coordinate with customers' GxP compliance requirements and their work on supplier evaluation and matters pertaining to agreements. Tencent Cloud will also present its ISO 9001 certification to customers upon request. For more information, see Section 4.5 "Supplier management".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 13	System	Before being used, every computerized system should be thoroughly tested to ensure that the system can function as intended. When a computerized system replaces a manual system, the two systems (manual and computerized) can function in parallel as part of testing and validation activities.	Customers should determine the scope and degree of validation based on the risk assessment results to ensure that the system functions as intended. Tencent Cloud implements product and service quality and security management throughout the system development lifecycle and ensures that all relevant components pass the comprehensive quality and security tests. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation".
Article 14	System	Systems can be accessed and used only by authorized personnel. Organizations should take appropriate measures to prevent unauthorized access to and use of their system. Procedures for authorization, cancellation, and authorization changes should be established for access to and use of the system. When necessary, consideration should be given to the ability of the system to track unauthorized access attempts. For any defects in the system beyond control of the personnel, there must be written procedures, records, and appropriate physical isolation means to ensure that the system is used only by authorized personnel.	Customers should take identity authentication and access control measures to ensure that access to their GxP business systems is under control and to prevent unauthorized access. They should also set the log feature according to the importance of the system. Tencent Cloud provides a wealth of identity authentication and access control products and tools and adopts various identity authentication and access control measures to ensure that backend operations is authorized, and logs are kept for security audits. For more information, see Section 5.8 "Identity authentication and access control". The log feature needs to be enabled for Tencent Cloud products and supporting systems, including but not limited to system logs

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			and application logs. The login activities and user operations related to backend operations are monitored, and logs are generated through the security components. For more information, see Section 5.2 "Logs and audit trails".
Article 15	System	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. When necessary, systems should include appropriate built-in checks of the correct and secure entry and processing of data.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should take measures to ensure the accuracy of manually entered data.
Article 16	System	Computerized systems should record the identities of those who enter or verify key data. Only authorized personnel may alter the entered data. Any alteration of the entered key data should be approved in advance, and the reason for the alteration should be documented. Consideration should be given, based on a risk assessment, to building into the system the creation of a record of data input and modifications as well as system use and changes.	Customers should establish the procedures for record access control and permission change review and keep system logs for audits. Tencent Cloud provides various identity authentication and access control measures and exercises strict access controls for backend operations. For more information, see Section 5.8 "Identity authentication and access control". The log feature needs to be enabled for Tencent Cloud products and supporting systems, including but not limited to system logs and application logs. The login activities and user operations related to backend opertions are monitored, and logs are generated through the security components. For more information, see Section 5.2 "Logs and audit trails".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 17	System	Any changes to a computerized system should be made in accordance with defined procedures, including evaluation, validation, review, approval, and implementation procedures. Such changes should be approved by competent personnel involved with the computerized system and be documented.	Customers should ensure that control processes and operation specifications are in place for any changes to their GxP systems. Tencent Cloud has established strict change and configuration management processes for its products and supporting platforms. It ensures that changes are secure and controllable through the change management platform. For more information, see Section 5.3 "Change and configuration management".
Article 18	System	In the case of the coexistence of electronic data and paper records, it should be clarified which should count as the master data.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should make decisions based on their own needs and comply with the applicable regulations.
Article 19	System	For electronic data to count as the master data, the following requirements should be met: (1) For the purpose of quality audits, the stored electronic data should be able to be printed into legible documents. (2) Data security must be guaranteed by physical or electronic means to prevent intentional or accidental corruption. During routine Ops or in case of any changes to the system (e.g. computer equipment or programs), the accessibility and integrity of the stored data should be checked.	Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data. Tencent Cloud provides data protection mechanisms and products to help customers protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		(3) Procedures for data backup and restoration should be established. Regular backups of all data should be done to protect the stored data for future use. Backups should be stored in a separate and secure location, and the retention period should at least meet the document and record retention requirements set out in this GMP.	
Article 20	System	Organizations should develop contingency plans that can be activated if a system failure occurs. How quickly a contingency plan is activated should depend on the urgency of the need to use the plan. For example, information that affects product recalls should be made available in a timely manner.	Customers should develop business continuity plans and carry out exercises for GxP systems on the basis of business impact analysis to ensure the effectiveness. Tencent Cloud has established a business continuity management system and developed contingency plans for its products and services. It will also coordinate with customers on their business continuity plans. For more information, see Section 5.10 "Business continuity management".
Article 21	System	Procedures for handling system failures or damage should be established and should be validated when necessary. All incidents, including system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis for corrective and preventive actions.	Customers should establish an incident management process and take appropriate corrective and preventive actions. Tencent Cloud has established a complete incident response process to ensure that incidents are dealt with promptly to mitigate any negative impact. If an incident may affect the customers' businesses, Tencent Cloud will inform the customers as soon as possible and provide suggestions on incident handling. For more information, see Section 5.9 "Incident response".

Appendix 1 "Computerized Systems" to Good Manufacturing Practice for Drugs by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 22	System	When a computerized system is used for batch release, the system should clearly identify and record the person releasing the batches.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable regulations on product release.
Article 23	Electronic signature	For Electronic data, electronic signatures may be used, provided that they meet the requirements of the applicable laws and regulations.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations using electronic signatures should comply with the applicable regulations.

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 4	General provisions	Records can be classified into different types according to their purpose, such as ledgers, logs, identifiers, processes, and reports. One or more types of records may be adopted based on the needs to ensure the authenticity, accuracy, integrity, and traceability of information throughout the process of drug development, production, operations, and use. One or more forms of media may be adopted for records, including paper, electronic, or both.	Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data. Tencent Cloud provides data protection mechanisms to help customers protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".
Article 5	General provisions	Where a computer (computerized) system is used to generate records or data, appropriate administrative and technical measures should be taken to ensure the authenticity, accuracy, integrity, and traceability of the generated information.	Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data. Tencent Cloud provides data protection mechanisms to help customers protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".
Article 6	General provisions	Electronic records should at least serve the same functions as the original paper records to meet the requirements for management on the go. In the case of the coexistence of electronic records and paper records, which serves as a baseline should be clarified in the procedures and management systems.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations using paper records should comply with the applicable regulations.

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 7	General provisions	A record management procedure should be established according to the purpose, type, and form of records. The responsibilities for record management should be clarified, and record controls be regulated.	Customers should establish a data or record management procedure and define the management responsibilities and control requirements for various types of data. Tencent Cloud has established a data security protection management procedure and specification. For more information, see Section 6.1 "Procedure for electronic records and data management".
Article 8	General provisions	Activities such as data collection, processing, storage, generation, retrieval, and reporting should meet the requirements for documenting or entering the corresponding type of data. The authenticity, accuracy, integrity, and traceability of data should be guaranteed.	Customers should establish a data or record management procedure and define the management responsibilities and control requirements for various types of data. Tencent Cloud has established a data security protection management procedure and specification. For more information, see Section 6.1 "Procedure for electronic records and data management".
	General provisions	According to the source and purpose, data can be divided into basic data, behavioral data, metering data, electronic data, and other types of data. Appropriate administrative and technical measures should be adopted for different types of data.	This requirement does not apply to Tencent Cloud. Customers should classify their GxP business data according to the source and purpose and take appropriate measures to manage the data.

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 10	General provisions	Personnel engaged in record and data management should receive necessary training, learn about the management requirements and skills, and abide by the professional code of ethics.	Customers should ensure that the personnel involved with GxP systems have the necessary system and procedure operation skills and qualifications. Tencent Cloud has established and implemented personnel training mechanisms to ensure that its personnel have the required qualifications, abilities, and awareness of information security. For more information, see Section 4.4 "Personnel management".
Article 11	General provisions	Records and data generated by a third party through the contract should meet the requirements herein. The management responsibilities of both parties should be clearly defined.	Customers are obligated to evaluate supplier qualifications and sign agreements with the suppliers to clearly define the responsibilities of both parties. As a cloud service provider, Tencent Cloud will coordinate with customers' GxP compliance requirements and matters pertaining to agreements. For more information, see Section 4.5 "Supplier management".
Article 20	Requirements for electronic records management	Computer (computerized) systems used for electronic records should meet the following requirements for hardware and software specifications: (1) Installation at a suitable location to prevent any disturbances from external environmental factors; (2) A server that supports the normal operations of the system;	Based on the selected cloud service mode, customers should ensure that their GxP computerized systems meet the applicable security requirements for the server, network, applications, devices, and specifications. Tencent Cloud has in place management processes and technical measures to guarantee the security and reliability of

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	Domain	GxP Requirements	Applicability and Section
		(3) A stable and secure network environment and a reliable information security platform; (4) A local area network environment for information transfers and data sharing between departments and positions; (5) Application software and databases that meet the applicable legal requirements and management needs; (6) Terminal devices and peripherals used to perform record operations; and (7) Technical materials such as an operation guide and drawings.	the underlying infrastructure. For more information, see Sections 5.4 "Physical security", 5.5 "Network security", 5.6 "Server security", and 5.7 "Application security".
Article 21	Requirements for electronic records management	Computer (computerized) systems used for electronic records should at least meet the following functional requirements: (1) The authenticity, accuracy, and consistency of the recording time and the system time should be guaranteed; (2) The system can display all data in the electronic records, and the generated data should be readable and printable; (3) The data generated by the system should be backed up regularly, the backup and data restoration processes must be validated, and data backup or deletions should be documented; and (4) In case of system changes, upgrade, or retirement, appropriate measures should be taken to ensure that the data in the original system can be viewed and traced during the retention period.	Customers should ensure the authenticity, accuracy, integrity, and availability of electronic records stored in computerized systems. Tencent Cloud provides data backup services for customers based on product features and manages changes to its products and supporting platforms in strict accordance with the change management process. For more information, see Sections 5.1 "Data backup and restoration" and 5.3 "Change and configuration management".

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
Article 22	Requirements for electronic records management	Permissions and login management should be implemented for electronic records, which includes but is not limited to the following: (1) Different permissions should be set for operations and system management. The user permissions assigned to the person in charge of the business process should be aligned with their responsibilities. They may not be granted system admin permissions (including the operating system, applications, and databases); (2) User permissions can be set and assigned, and permission modifications can be tracked and queried; (3) The uniqueness and traceability of the logged-in user should be guaranteed, and electronic signatures should be used in accordance with the Electronic Signature Law of the People's Republic of China; and (4) Information about system operations should be documented, including but not limited to the operator, operation time, operation process, and reason for the operation; data generation, modification, deletion, reprocessing, renaming, and transfer; and changes or modifications to the settings, configurations, parameters, and timestamp of the computerized system.	Customers should take identity authentication and access control measures to ensure that access to their GxP business systems is under control and to prevent unauthorized access. Tencent Cloud provides a wealth of identity authentication and access control products and tools and adopts various identity authentication and access control measures to ensure that backend operations is authorized, and logs are kept for security audits. For more information, see Section 5.8 "Identity authentication and access control".
Article 23	Requirements for electronic records management	In validation of computerized systems used for electronic records, the scope and degree of validation should be determined based on multiple factors such as the system's infrastructure, system and business features, and comprehensive system maturity and complexity, so as to ensure that the system functions as intended.	Customers should determine the scope and degree of validation based on the risk assessment results to ensure that the system functions as intended. Tencent Cloud implements product and service quality and security management throughout the system development lifecycle and ensures that all relevant components remain in

Requirements for Drug Records and Data Management (Trial) by the National Medical Products Administration of China			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
			a valid state. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation".
Note: The provisions on paper-based records and business data management in the Requirements for Drug Records and Data Management (Trial) do not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable requirements for business operations.			

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	Domain	GxP Requirements	Applicability and Section
820.5	Quality management	Each manufacturer shall establish and maintain a quality system that is appropriate for the specific medical device(s) designed or manufactured, and that meets the requirements of this part.	Customers should establish and maintain a quality management system. Tencent Cloud has established a quality management system based on international standards, which has been certified by authoritative third-party certification bodies. For more information, see Sections 4.1 "Quality management system" and 4.2 "Quality management audit".
820.20	Quality management	(a) Quality policy. Management with executive responsibility shall establish its policy and objectives for and commitment to quality. Management with executive responsibility shall ensure that the quality policy is understood, implemented, and maintained at all levels of the organization. (b) Organization. Each manufacturer shall establish and maintain an adequate organizational structure to ensure that devices are designed and produced in accordance with the requirements of this part. (1) Responsibility and authority. Each manufacturer shall establish the appropriate responsibility, authority, and interrelation of all personnel who manage, perform, and assess work affecting quality, and provide the independence and authority necessary to perform these tasks. (2) Resources. Each manufacturer shall provide adequate resources, including the assignment of trained personnel, for management, performance of work, and	Customers should establish and maintain a quality management system. Tencent Cloud has established a quality management system based on international standards, which has been certified by authoritative third-party certification bodies. For more information, see Sections 4.1 "Quality management system" and 4.2 "Quality management audit".

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	Domain	GxP Requirements	Applicability and Section
		assessment activities, including internal quality audits, to meet the requirements of this part. (3) Management representative. Management with executive responsibility shall appoint, and document such appointment of, a member of management who, irrespective of other responsibilities, shall have established authority over and responsibility for: (i) Ensuring that quality system requirements are effectively established and effectively maintained in accordance with this part; and (ii) Reporting on the performance of the quality system to management with executive responsibility for review. (c) Management review. Management with executive responsibility shall review the suitability and effectiveness of the quality system at defined intervals and with sufficient frequency according to established procedures to ensure that the quality system satisfies the requirements of this part and the manufacturer's established quality policy and objectives. The dates and results of quality system reviews shall be documented. (d) Quality planning. Each manufacturer shall establish a quality plan which defines the quality practices, resources, and activities relevant to devices that are designed and manufactured. The manufacturer shall establish how the requirements for quality will be met.	

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		(e) Quality system procedures. Each manufacturer shall establish quality system procedures and instructions. An outline of the structure of the documentation used in the quality system shall be established where appropriate.	
820.22	Quality audit	Each manufacturer shall establish procedures for quality audits and conduct such audits to assure that the quality system is in compliance with the established quality system requirements and to determine the effectiveness of the quality system. Quality audits shall be conducted by individuals who do not have direct responsibility for the matters being audited. Corrective action(s), including a reaudit of deficient matters, shall be taken when necessary. A report of the results of each quality audit, and reaudit(s) where taken, shall be made and such reports shall be reviewed by management having responsibility for the matters audited. The dates and results of quality audits and reaudits shall be documented.	Customers should establish and maintain a quality management system and conduct audits on the system. Tencent Cloud has established a quality management system based on international standards, which has been certified by authoritative third-party certification bodies. For more information, see Sections 4.1 "Quality management system" and 4.2 "Quality management audit".
820.25	Personnel	(a) General. Each manufacturer shall have sufficient personnel with the necessary education, background, training, and experience to assure that all activities required by this part are correctly performed. (b) Training. Each manufacturer shall establish procedures for identifying training needs and ensure that all personnel are trained to adequately perform their assigned responsibilities. Training shall be documented. (1) As part of their training, personnel shall be made aware of device defects which may occur from the improper performance of their specific jobs.	Customers should ensure that the personnel involved with GxP systems have the necessary system and procedure operation skills and qualifications. Tencent Cloud has established and implemented personnel training mechanisms to ensure that its personnel have the required qualifications, abilities, and awareness of information security. For more information, see Section 4.4 "Personnel management".

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
		(2) Personnel who perform verification and validation activities shall be made aware of defects and errors that may be encountered as part of their job functions.	
820.40	Document controls	Each manufacturer shall establish and maintain procedures to control all documents that are required by this part. The procedures shall provide for the following: (a) Document approval and distribution. Each manufacturer shall designate an individual(s) to review for adequacy and approve prior to issuance all documents established to meet the requirements of this part. The approval, including the date and signature of the individual(s) approving the document, shall be documented. Documents established to meet the requirements of this part shall be available at all locations for which they are designated, used, or otherwise necessary, and all obsolete documents shall be promptly removed from all points of use or otherwise prevented from unintended use. (b) Document changes. Changes to documents shall be reviewed and approved by an individual(s) in the same function or organization that performed the original review and approval, unless specifically designated otherwise. Approved changes shall be communicated to the appropriate personnel in a timely manner. Each manufacturer shall maintain records of changes to documents. Change records shall include a description of the change, identification of the affected documents, the signature of the approving individual(s), the approval date, and when the change becomes effective.	Customers should put in place a document management procedure to regulate the standard operating procedures (SOPs) and the procedures regarding system operations and maintenance to ensure the accuracy and effectiveness of documents. Tencent Cloud has established a document management procedure covering all stages from document preparation, approval, and release to storage, use, and revision to retention and invalidation. This procedure is designed for unified management of documents across various management systems. For more information, see Section 4.3 "Document management".

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
820.50	Purchasing controls	Each manufacturer shall establish and maintain procedures to ensure that all purchased or otherwise received product and services conform to specified requirements. (a) Evaluation of suppliers, contractors, and consultants. Each manufacturer shall establish and maintain the requirements, including quality requirements, that must be met by suppliers, contractors, and consultants. Each manufacturer shall: (1) Evaluate and select potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements, including quality requirements. The evaluation shall be documented. (2) Define the type and extent of control to be exercised over the product, services, suppliers, contractors, and consultants, based on the evaluation results. (3) Establish and maintain records of acceptable suppliers, contractors, and consultants. (b) Purchasing data. Each manufacturer shall establish and maintain data that clearly describe or reference the specified requirements, including quality requirements, for purchased or otherwise received product and services. Purchasing documents shall include, where possible, an agreement that the suppliers, contractors, and consultants agree to notify the manufacturer of changes in the product or service so that manufacturers may determine whether the changes may affect the quality of a finished device. Purchasing data shall be approved in accordance with § 820.40.	Customers are obligated to evaluate supplier qualifications and sign agreements with the suppliers to clearly define the responsibilities of both parties. As a cloud service provider, Tencent Cloud will coordinate with customers' GxP compliance requirements and their work on supplier evaluation and matters pertaining to agreements. Tencent Cloud will also present its ISO 9001 certification to customers upon request. For more information, see Section 4.5 "Supplier management".
Note: Other requirements in Part 820 do not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable requirements for business operations.			

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
11.10 (a)	Electronic Records; Electronic Signatures – Controls for closed systems	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Customers should determine the scope and degree of validation based on the risk assessment results to ensure that the system functions as intended. Tencent Cloud implements product and service quality and security management throughout the system development lifecycle and ensures that all relevant components remain in a valid state. For more information, see Sections 4.6 "System development lifecycle" and 4.7 "Validation".
11.10 (b)	Electronic Records; Electronic Signatures – Controls for closed systems	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data. Tencent Cloud provides a range of data protection mechanisms and products to empower customers to protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".
11.10 (c)	Electronic Records; Electronic Signatures –	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data.

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	Domain	GxP Requirements	Applicability and Section
	Controls for closed systems		Tencent Cloud provides a range of data protection mechanisms and products to empower customers to protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".
11.10 (d)	Electronic Records; Electronic Signatures – Controls for closed systems	Limiting system access to authorized individuals.	Customers should take identity authentication and access control measures to ensure that access to their GxP business systems is under control and to prevent unauthorized access. Tencent Cloud provides a wealth of identity authentication and access control products and tools and adopts various identity authentication and access control measures to ensure that backend operations is authorized, and logs are kept for security audits. For more information, see Section 5.8 "Identity authentication and access control".
11.10 (e)	Electronic Records; Electronic Signatures – Controls for closed systems	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Customers should ensure that the system retains logs for the purpose of audit trails. Tencent Cloud has established a log management system. It records the logs of backend operations and carries out audits periodically. For more information, see Section 5.2 "Logs and audit trails".

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	**Domain**	**GxP Requirements**	**Applicability and Section**
11.10 (f)	Electronic Records; Electronic Signatures – Controls for closed systems	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable regulations.
11.10 (g)	Electronic Records; Electronic Signatures – Controls for closed systems	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Customers should take identity authentication and access control measures to ensure that access to their GxP business systems is under control and to prevent unauthorized access. Tencent Cloud provides various identity authentication and access control measures and exercises strict access controls for backend operations. For more information, see Section 5.8 "Identity authentication and access control".
11.10 (h)	Electronic Records; Electronic Signatures – Controls for closed systems	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable regulations.

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	Domain	GxP Requirements	Applicability and Section
11.10 (i)	Electronic Records; Electronic Signatures – Controls for closed systems	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Customers should ensure that the personnel involved with GxP systems have the necessary system and procedure operation skills and qualifications. Tencent Cloud has established and implemented personnel training mechanisms to ensure that its personnel have the required qualifications, abilities, and awareness of information security. For more information, see Section 4.4 "Personnel management".
11.10 (j)	Electronic Records; Electronic Signatures – Controls for closed systems	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	This requirement does not apply to Tencent Cloud. GxP-regulated healthcare organizations using electronic signatures should comply with the applicable regulations.
11.10 (k)	Electronic Records; Electronic Signatures – Controls for closed systems	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Customers should put in place a document management procedure to regulate the standard operating procedures (SOPs) and the procedures regarding system operations and maintenance to ensure the accuracy and effectiveness of documents. Tencent Cloud has established a document management procedure covering all stages from document preparation,

<table>
<tr><th colspan="4">Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)</th></tr>
<tr><th>No.</th><th>Domain</th><th>GxP Requirements</th><th>Applicability and Section</th></tr>
<tr><td></td><td></td><td></td><td>approval, and release to storage, use, and revision to retention and invalidation. This procedure is designed for unified management of documents across various management systems. For more information, see Section 4.3 "Document management".</td></tr>
<tr><td>11.30</td><td>Electronic Records; Electronic Signatures – Controls for open systems</td><td>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</td><td>Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data.
Tencent Cloud provides a range of data protection mechanisms and products to empower customers to protect the integrity, availability, and confidentiality of their data. For more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".</td></tr>
<tr><td colspan="4">Note: Sections 11.50-11.300 do not apply to Tencent Cloud. GxP-regulated healthcare organizations using electronic signatures should comply with the applicable regulations.</td></tr>
<tr><td>211.68 (b)</td><td>Automatic, mechanical, and electronic equipment</td><td>Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system. A backup file of data entered into the computer or</td><td>Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data.
Tencent Cloud provides a range of data protection mechanisms and products to empower customers to protect the integrity, availability, and confidentiality of their data. For</td></tr>
</table>

Title 21 of the Code of Federal Regulations (21 CFR) by the U.S. Food and Drug Administration (FDA)			
No.	Domain	GxP Requirements	Applicability and Section
		related system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances a written record of the program shall be maintained along with appropriate validation data. Hard copy or alternative systems, such as duplicates, tapes, or microfilm, designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained.	more information, see Sections 5.1 "Data backup and restoration" and 6 "Electronic Records and Data Management".
Note: Other requirements in Part 211 do not apply to Tencent Cloud. GxP-regulated healthcare organizations should comply with the applicable requirements for business operations.			