

Compliance

International Authority

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

International Authority

ISO 27001 Certification

ISO 27017 Guidelines for Cloud Service Information Security Control Implementation

CSA STAR Certification

ISO 20000 Certification

ISO 22301 Certification

ISO 9001 Certification

SOC Audit

International Authority ISO 27001 Certification

Last updated : 2020-05-15 12:03:02

ISO 27001 is a management system that, at its core, revolves around information assets and business risk management. It calls for stringent requirements in the setting up, implementation and documentation of a corporation's information security management. The predecessor of the ISO 27001 is the BS 7799 Information Security Management System Standard, which was drafted by the authoritative standards development and international certification provider, BSI. Subsequently, the latter was adopted by the International Organization for Standardization (hereinafter "ISO"), and refined as the ISO 27001. The ISO 27001 has since become the most rigorous and recognized - as well as extensively accepted and applied - prevailing global system certification standard in respect of information security.

In recent years, emerging IT technologies have developed rapidly worldwide, bringing along with it new security threats. As such, the ISO organization took the step to formally upgrade the ISO 27001:2005 to the ISO 27001:2013. Comparatively, the former is more applicable to traditional IT frameworks, while the latter supplements the information security management requirements pertaining to new technologies that are lacking in the 2005 edition. What this means, is that the ISO 27001:2013 certification is better placed to reflect the industry's commitment to security and indicates that information security management for corporations is now equipped with an established scientific and effective system of management which better enables the corporation to provide users with reliable information services. At present, a number of governmental organizations, banks, securities, insurance, telecommunications and internet companies both domestic and foreign as well as various multinational corporations have all incorporated this ISO standard, so as to manage their information security in a systemic manner.

ISO 27017 Guidelines for Cloud Service Information Security Control Implementation

Last updated : 2019-12-30 09:53:25

ISO 27017:2015 is an international standard issued by the International Organization for Standardization (ISO) in December 2015. It is a practical standard for cloud service information security and offers cloud service providers and customers with guidelines for specific security controls and their implementation. ISO 27017 is a standard based on ISO 27002, and its primary purpose is to provide cloud vendors with security specifications for cloud construction and OPS. The requirements in ISO 27017 consist of the following two parts:

- Requirements in ISO 27002: under the framework of ISO 27002, additional implementation guidelines for 37 controls are proposed.
- Special requirements in cloud environments: outside the framework of ISO 27002, 7 control measures that require special consideration in cloud computing environments are added.

Specificity of ISO 27017:

- On each control, implementation guidelines are provided to cloud service providers and customers respectively, and the roles and responsibilities of both parties are elaborated.
- Based on the requirements in the ISO 27017 standard, Tencent Cloud has established a more comprehensive cloud security management system to improve its overall cloud security service capabilities.

CSA STAR Certification

Last updated : 2018-06-22 10:04:41

The CSA Star, a cloud security assurance rating, is based on the Cloud Control Matrix (CCM) developed by the foremost international and non-profit organization, the Cloud Security Alliance. It satisfies specific cloud computing security sector requirements and is a global certification that targets the characteristics of cloud computing security. At the same time, it is an enhanced edition of the ISO/IEC 27001 Information Security Management System, and renders the problems unique to cloud security in a visual format, providing cloud service providers with an objective evaluation framework with regard to their security control capabilities.

Tencent Cloud has accumulated extensive experience in security issues over the years, and was conferred the CSA Star certification with a gold rating, in September 2016. At the same time, Tencent Cloud procured both the CNAS and UKAS domestic and overseas certification qualifications in relation to information security management system - the first ever cloud service provider to concurrently attain all these qualifications, further reinforcing its status as the pre-eminent cloud service provider in the country.

ISO 20000 Certification

Last updated : 2019-12-30 09:57:59

ISO20000 is derived from the BSI15000 standard, which itself was formulated by the British Standards Institute with regard to IT services management. The said standard dates back to 1995, and underwent several revisions before its current rendition, the ISO20000, a two-part information technology service management standard that has been widely accepted.

The ISO20000 IT Service Management System aims to provide a mode of establishing, implementing, operating, monitoring, evaluating, maintaining and improving IT service management systems; managing IT issues via “standardization of IT services”; as well as categorizing IT issues and identifying the inherent relationship between the issues. Thereafter, based on the service level, to plan, promote, monitor and reinforce communication with customers, in order to help the corporation set up an integrated system that is effective and revolves around the customer.

Tencent Cloud has successfully procured the ISO20000 certificate, the scope of which covers cloud computing, hosting and disaster-preparedness services among others.

ISO 22301 Certification

Last updated : 2020-05-15 12:03:40

ISO 22301 is an inaugural set of international standards focusing on Business Continuity Management, (hereinafter “BCM”), providing a comprehensive yet generic methodology that ensures enterprises are able to satisfy and comply with globally accepted best practices.

This certification is applicable across all types of industries and organizations, regardless of scale and nature. In addition, it is of particular pertinence to industries that are deemed “high-risk” and those that operate under a strict regulatory regime, including Finance, IT & Communications and Manufacturing. In the course of its business, an enterprise is often impacted by various internal as well as external factors. In drastic situations, this may even lead to a cessation in operations, which if unforeseen, may result in severe losses.

Business Continuity Management is currently gaining in prominence, with the finance industry as a fine example. Since 2005, when the State Council promulgated the Response Plan for Financial Emergencies, a state-level policy, the said industry has progressively sought to incorporate BCM into its regulatory ambit. The China Banking Regulatory Commission as well as the China Insurance Regulatory Commission (amongst other Regulatory Commissions) have also successively introduced requirements pertaining to BCM for the finance industry.

ISO 9001 Certification

Last updated : 2020-05-19 19:52:21

ISO 9001 Certification

Transformed from the world's first quality management system BS 5750 (developed by BSI), ISO 9001 is a globally recognized quality management framework. As a systematic guide and standard for guaranteeing the product quality and operations of companies, it takes care of the whole process of products and services from planning and implementation to improvement and operation, ensuring that customer needs and applicable laws and regulations are met.

By using a quality management system, you can effectively and efficiently achieve the expected quality goals. You should take corrective and preventive measures and continuously improve the effectiveness of the quality management system based on the review and management of the system. This process is fundamental to the development of your business.

SOC Audit

Last updated : 2020-05-19 19:52:21

SOC Audit

The System and Organization Controls (SOC) report is an independent audit report for security, availability, and confidentiality control checkpoints of the Tencent Cloud platform. The report provided to you and your auditors will be adjusted according to the types of attestation services in order to meet specific needs.

SOC reports are a series of reports related to internal controls of a service organization issued by professional third-party accounting firms in compliance with the applicable guidelines of the American Institute of Certified Public Accountants (AICPA).

- Based on AT-C Section 320 in AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Tencent Cloud SOC 1 report is issued for the control environment of the Tencent Cloud service system, which is related to the internal controls over your financial statements.
- Based on AT-C Section 205 and TSP Section 100 (2017 version) in AICPA SSAE No. 18, Tencent Cloud SOC 2 and 3 reports are independent reports assessing the adequacy of the controls and design related to the security, availability, and confidentiality of the Tencent Cloud service system. AICPA released the latest 2017 version of the trust services criteria in April 2017 and specified that during the transition period of the new criteria (from April 15, 2017 to December 15, 2018), service providers could choose whether to follow the latest 2017 version or the legacy 2016 version of the criteria. As a leading cloud service provider, Tencent Cloud adopted the 2017 version of the trust services criteria during the SOC audit in 2017, becoming the first provider in China to follow the 2017 version.

The SOC reports can provide Tencent Cloud users with valuable information to evaluate and resolve risks related to the service organization:

- SOC 1 report: Tencent Cloud user organizations and their independent auditors can evaluate major misstatement risks of their financial statements based on the SOC 1 report and their internal controls.
- SOC 2 report: Tencent Cloud user organizations, independent auditors, regulators, shareholders, and other stakeholders can evaluate the design adequacy and operational effectiveness of Tencent Cloud's internal controls (covering security, availability, process integrity, confidentiality, and privacy) based on the SOC 2 report.

- SOC 3 report: it is a part of the SOC 2 report, which mainly describes the Tencent Cloud service system. The report can be made available to the public upon request. The public can learn more about Tencent Cloud's internal controls in the SOC 3 report.