Compliance

Region and Industry Recognition

Product Documentation

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

Region and Industry Recognition

OSPAR

Last updated : 2020-08-13 17:07:22

Tencent Cloud has achieved the Outsourced Service Provider’s Audit Report (OSPAR) attestation on June 9th, 2020 for multiple products and services in the Singapore region. OSPAR is the outsourcing standard for the Singapore financial industry. Achieving this attestation demonstrates that Tencent Cloud’s security capabilities meet the stringent requirements for financial services in Singapore and even Southeast Asia.

The OSPAR assessment is performed by an independent third-party auditor in accordance with the Guidelines on Control Objectives and Procedures for Outsourced Service Providers (ABS Guidelines) established by the Association of Banks in Singapore. These guidelines are based on the Singapore Standards on Assurance Engagement (SSAE 3000) and intended to assist financial institutions in assessing the capability of their outsourced service providers in three aspects, entity level controls, general information technology controls and service controls. OSPAR is recognized by the Monetary Authority of Singapore (MAS) and meets their compliance requirements.

Tencent Cloud’s alignment with the ABS guidelines demonstrates that Tencent Cloud’s overseas services have achieved financial-grade security controls, securing our position as a leading global cloud service provider.

KISMS

Last updated : 2020-02-19 11:13:01

Tencent Cloud has achieved the Korean Information Security Protection Management System (K-ISMS) certification, proving that the information security management systems and capabilities developed by Tencent Cloud are in compliance with applicable Korean laws and standards.
The K-ISMS certification is a Korean government-backed certification sponsored by the Korea Internet & Security Agency (KISA) and affiliated with the Korean Ministry of Science and ICT (MSIT). It aims to help Korean organizations consistently and securely protect their information assets based on applicable Korean laws on information and communication technology. As a Korea-specific information security protection framework, K-ISMS defines a set of strict control requirements that cover asset management, access control, authentication and permission management, encryption, and disaster recovery, with a focus on auditing the security and reliability of organizations' management of key information assets, including organizational and personal information.
Achieving this certification means that Tencent Cloud customers in Korea can easily demonstrate adherence with local legal requirements to protect key digital information assets and meet KISA compliance standards with greater ease. This also reflects that Tencent Cloud’s information security protection strategies and threat handling procedures effectively minimizes the impact of any security breaches.

HIPAA

Last updated : 2020-02-19 11:12:36

HIPAA

The Health Insurance Portability and Accountability Act was enacted in 1996 in the United States. One of its purposes is to promote the use of electronic health records in order to improve the efficiency and quality of the healthcare system by strengthening information sharing. HIPAA also protects the security (including availability, integrity, and confidentiality) and privacy of Protected Health Information (PHI) during information creation, receipt, maintenance, and transfer by related entities and their business associates. HIPAA-covered entities and their business associates are required to take appropriate security measures when processing, maintaining, and storing PHI.

For Tencent Cloud services, PHI is an electronic form which we refer to as electronic Personal Health Information (ePHI). ePHI contains a very wide range of health data and related data that can be used to identify individuals.

Tencent Cloud releases self-assessment reports for HIPAA compliance, which explain its ability to protect users' personal information and the effectiveness of the control measures taken.

MTCS

Last updated : 2020-02-19 11:13:18

Tencent Cloud has achieved the Singapore Multi-Tier Cloud Security Standard Level-3 certification. The MTCS Standard is developed under the Information Technology Standards Committee (ITSC) of the Infocomm Development Authority of Singapore (IDA). The ITSC promotes and facilitates national programs to standardize IT and communications, and Singapore’s participation in international standardization activities.
MTCS has different levels of cloud security standard. Level 1 covers basic security. Level 2 adds a set of stringent management and tenant control. Level 3 addresses reliability and recoverability needs for efficient information systems. MTCS builds upon recognized international standards such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, availability, business continuity, disaster recovery, and incident management. MTCS is a common cloud standard that cloud service providers (CSPs) can apply to address customer concerns regarding cloud-based data security and confidentiality, and the impact on businesses using cloud services. It also provides verifiable operational transparency and visibility for risks customer face when using cloud services.

The Motion Picture Association of America (MPAA)

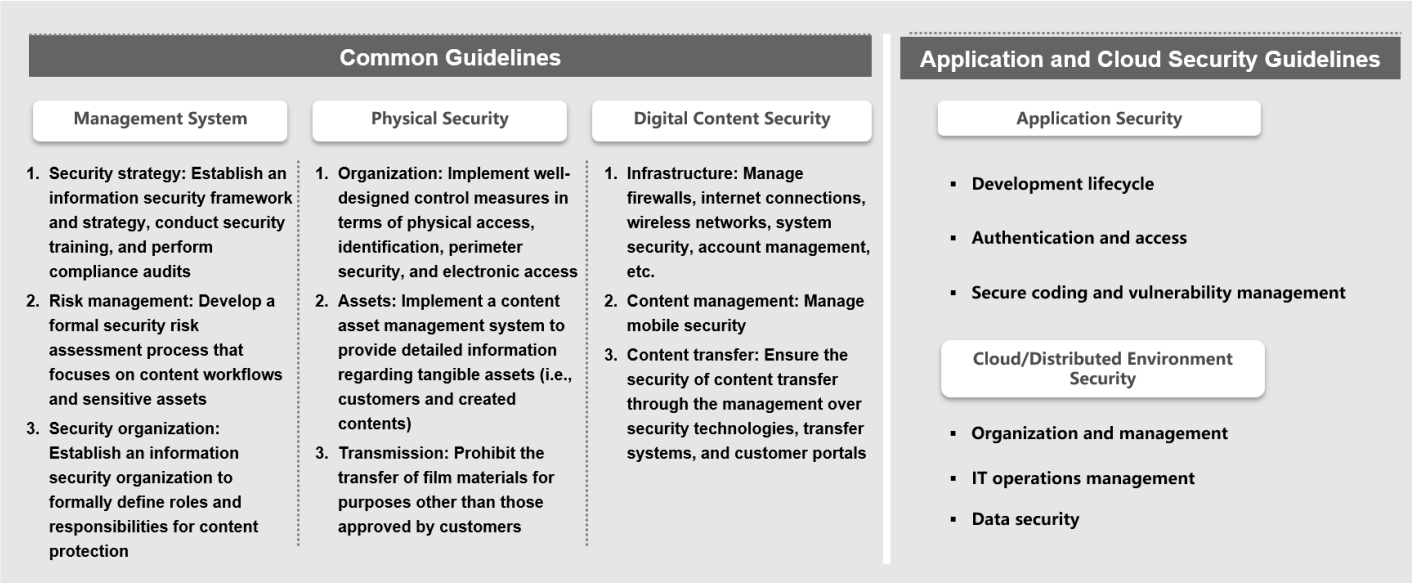
Last updated : 2019-06-12 15:20:13

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. These best practices are designed to inform application and cloud service providers collaborating with MPAA members the content security requirements. Media companies use these best practices to assess risk and security of their content. Tencent Cloud ensures that its management of customer content is in compliance with the MPAA Content Security Model through self-assessment.

The components of the model are based on the relevant ISO standards (27001-27002), security standards (i.e. NIST, CSA, ISACA, and SANS), and industry best practices. Among them, ISO27001, ISO27017, ISO27018, PCI DSS and CSA STAR are key compliance programs of Tencent Cloud for which it has passed third-party audits.

Overview of MPAA Standards

MPAA's best practice standards, including *Content Security Best Practices - Common Guidelines* and *Content Security Best Practices - Application and Cloud/Distributed Environment Security Guidelines*, provide guidance on the best practice controls and implementation steps.



For more information, visit MPAA's official website

PCI DSS Certification

Last updated : 2018-06-22 10:12:35

The Payment Card Industry Data Security Standard (“PCI DSS”) is created and maintained by the Payment Card Industry Security Standards Council (“PCI SSC”). The PCI SSC was formed in the Autumn of 2006, via the collective efforts of five global payment brands, namely American Express, Discover Financial Services, JCB, Mastercard Worldwide and Visa, and, is a unified and professional information security standards council.

The PCI DSS, also known as the Payment Card Industry (PCI) Data Security Standard, is the sole and definitive global payment card industry data security standards. In order to boost the data security of cardholders, the PCI DSS sets out a uniform benchmark worldwide for the technology and operating requirements with regard to protection of account data. The scope of application extends from entities involved in card processing, such as merchants, processors, acquiring bank/ organizations, card issuers and service providers to other entities involved in the storing, processing or transmitting of the cardholder’s data.

Tencent Cloud has already passed the review of the PCI DSS certification, and has attained the qualification of a PCI DSS Grade 1 service provider. Building on the foundation of the PCI DSS V3.2 certification standard and norms, the PCI DSS Cloud Computing Guidelines V2.0 have since been released, with an especial focus on cloud computing. Tencent Cloud, in collaboration with third party testing and assessing organization ATSEC, provides secure and compliant services and ensures users of Tencent Cloud can enjoy a secure and reliable paid-service worldwide.

CYBERSECURITY CLASSIFIED PROTECTION

Last updated : 2018-06-22 10:11:47

What is Cybersecurity Classified Protection?

Section 21 of the Cybersecurity Law of the People's Republic of China (which came into force on 1 June 2017), states that, "China [shall] implement a cybersecurity classified protection system". This said cybersecurity classified protection is a rudimentary system aimed at protecting the cybersecurity of China and is also a fundamental safeguard in the protection of information development and maintenance of information security of the country. Cybersecurity protection consists of five categories (with Class V being the highest ranking), based on factors such as the importance of the information system in relation to national security, economic development and social and daily life as well as the extent of the detriment to national security, social order, public interest and citizens, corporations and other organizations when the same is damaged or impaired. Pursuant to cybersecurity classified protection criteria and relevant regulations, the Tencent Finance Cloud Platform has completed Class IV testing and registration, while Tencent Public Cloud as well as the Customer Service System, Billing System and Operations & Maintenance Management System for the Tencent Cloud Platform, have completed the testing and registration under Class III.

What are the implications of the Cybersecurity Classified Protection Assessment?

1. Facilitates Classified Protection Compliance by Cloud Users

According to the cybersecurity classified protection, information systems of varying security classes should be equipped with differing levels of security protection capabilities. With the conclusion of cybersecurity classified protection evaluation for Tencent Cloud, it represents that Tencent Cloud has and will strictly adhere to the national technical protection and security management requirements in relation to cloud computing platform security development. As such, it is able to render to corporate users across industries and business lines services that facilitate classified protection compliance. Further, Tencent Cloud is able to assist corporations in providing proof of secure cloud platform operations during the evaluation of their classified protection compliance as well as to provide corporate users with enhanced security capabilities that are necessary for business systems, so as to satisfy the classified protection compliance requirements.

2. Convenient and Faster Classified Protection Assessment for Cloud Users

For users of cloud services, when undergoing evaluation on cybersecurity classified protection, other than their own business systems and virtual resources (such as cloud hosting, cloud database and

cloud network) that manage operations and maintenance, it is not necessary to conduct a duplicate assessment with regard to the infrastructure provided by the cloud platform, thereby reducing complexity in the classified protection compliance process.

3. Protecting the Personal Information of Cloud Users

With the enactment of the Cybersecurity Law, the definition and relevant protection requirements pertaining to “personal information” have been clarified from a legal standpoint. Tencent Cloud has always placed much weight on the information protection of cloud users, and the Tencent Cloud classified protection naturally encompasses security capabilities in this respect.

ITSS Certification

Last updated : 2018-06-22 10:13:11

Tencent Cloud has been granted the Public as well as Private Cloud Service Capability Assessment Certificate as a mark of conformance.

Under the auspices of the Department of Information and Software Services, the China Electronic Industry Standardization Technology Association - Information Technology Service Standards Sub-Association (“ITSS”), has with reference to the General Requirements on Information Technology & Cloud Computing Service Operations and other state-level standards, constituted a third party testing and assessment organization to develop a pilot cloud computing service capability assessment, namely, the ITSS Cloud Computing Capability Assessment.

The said assessing organization conducts a multi-faceted evaluation on the service capabilities of participating corporations, based on this as well as other relevant national standards, and combined with crucial elements such as the cloud computing service personnel, technology, process and resources, in order to determine the capability grading achieved by the said corporations (during the pilot phase, participating corporations will only be graded as either basic or advance).

The ITSS obtained approval from the Ministry of Civil Affairs in June 2013, and was founded on 8 January 2014. It is an information technology services industry social group, comprising of volunteers from the information technology service industry supervisory departments, corporations, tertiary institutions, social groups, industry users and other relevant segments. Under the direction of the Ministry of Industry and Information Technology, the ITSS prepares and formulates information technology service standards, with the goal of driving technological and industry developments, adapting to market needs and ultimately, to realize the standardization and internationalization of the domestic information technology services.

Trusted Cloud Services Certification

Last updated : 2018-08-29 11:58:43

The Trusted Cloud Services (TRUCS) Certification is the sole recognized certification system pertaining to cloud services domestically. It was jointly developed by the Data Center Alliance and the Cloud Computing Development & Policy Forum. Based on scientific principles, the Trusted Cloud Services certification fully draws from overseas and practical domestic experience in the preparation of the following three standards, namely, the Cloud Computing Service Agreement Reference Framework, the Assessment Methodology for Trusted Cloud Services Certification and the Trusted Cloud Services Certification Modus Operandi. This is the first time an authoritative domestic organization has initiated a cloud services certification. The high bar it sets in relation to specifications and standards has called for even higher standards to be employed by the domestic cloud service operators, and has the effect of spurring the operating norms as well as the scale of the industry.

In accordance with the requirements of the Trusted Cloud Services certification, Tencent hosting services, database services, cloud cache services, cloud object storage services, local load balancing services, inter-data center VPN services, cloud delivery services and block storage services have all passed the assessment and obtained the certification from the Data Center Alliance. At the same time, Tencent Cloud was the initial batch of providers to satisfy the Trusted Cloud “Gold Class Operations” special assessment.

What does the evaluation for the Trusted Cloud Services certification comprise of?

In order to fully demonstrate the technical indicators and level of the cloud services providers, the “Trusted Cloud Services” certification comprises of three broad categories, 16 indicators and numerous items. The three main categories are data management, business quality and protection of rights and interests. The specific evaluation criteria includes the durability of data storage, whether data destruction, data migration, data confidentiality, data rights awareness and data review/ verification are available and to what degree, business function, business availability, business flexibility, failure recovery ability, network access performance, service accuracy metrics, changes in service, termination clause, service compensation clause, user termination clause as well as service provider indemnity clause.

What is the purpose and significance of the Trusted Cloud Services certification?

The content of the Trusted Cloud Services certification essentially encompasses 90% of the matters that service providers have to undertake to users or keep them apprised of (as per the SLA). The

said certification systematically evaluates to what degree the cloud service providers are able to implement and realize the 16 indicators, and users may make use of the results of the certification assessment to determine whether the undertakings of the cloud service provider are authentic and trustworthy.

Tencent Cloud has successfully obtained the Trusted Cloud Services certification, a testament to the fact that Tencent Cloud's undertakings as per the Service Level Agreement (SLA) and in relation to User Information Disclosure (including durability of data storage, data confidentiality, failure recovery ability, service availability etc.) meet the requirements demanded by the certification. It also attests to the user transparency provided as well as being a crucial benchmark which users may rely on to select a secure and trusted cloud service provider.

Business Lines that have been awarded the Trusted Cloud Service Provider Certification

Cloud Hosting No: 01018
Cloud Data Storage Services No: 03004
Cloud Cache Services No: 06001
Cloud Object Storage Services No: 02016
Local Load Balancing Services No: 10003
Inter-Data Center VPN Services No: 13001
Cloud Delivery Services No: 08014
Block Storage Services No: 05014
Private Cloud Segment No: H02010
Application Hosting Container No: 04011

Trusted Cloud "Gold Class Operations" Special Assessment

Certificate No: G01004

Trusted Cloud official website: https://www.kexinyun.org/

Big Data Product Capability Certification

Last updated : 2018-06-22 10:10:00

Data Center Alliance (www.dca.org.cn) was established on 16 January 2014, under the purview of the China Communications Standards Association, which is itself under the control of the Ministry of Industry and Information Technology. DCA embarked on the task of developing data centers, cloud computing, big data and mobile internet, based on the principles of practicality, fairness, effectiveness and shared collaboration.

For the time being, there are 6 constituent committees, namely, the Finance Committee, the Consulting Committee, the Open Data Center Committee, the Regional Liaison Committee, the Open Mobile Internet Committee and the IT Operations & Maintenance Committee as well as over a dozen working groups (Trusted Cloud, Cloud Insurance, Big Data, Green Conservation, IT Equipment, Infrastructure, Mobile Office, Mobile Healthcare, Biometric Identification, User, Server, Modular Data Center, Data Center Network and Intellectual Property).

Big Data Product Capability Certification entails seven metrics, namely functionality, operations & maintenance capability, multi-tenancy, availability, security, scalability and compatibility. There are a total of 37 indicators and the entity must undergo a rigorous four-pronged process of information review and verification, vendor-supplier evaluation, technology testing, and expert evaluation. Customers are able to benefit from reviewing features and capabilities of big data products that pass the stringent certification specifications, and are better poised to make a choice on what products to purchase and use. Currently, this certification has been elevated from a Data Center Alliance Standard to an Industry Standard. Tencent Cloud is the only large internet company in the pioneering batch of enterprises to be awarded the said certification.

CDN Qualification

Last updated : 2018-06-22 10:08:47

On 1 March 2016, the Telecommunication Business Classification Catalogue (2015 edition) was officially implemented. As compared to the preceding 2003 edition, this revision has a new Content Distribution Network (CDN) Business added to it, which has been classified in category 1 of the value-added telecommunication business, to be so managed. Incorporating CDN into the catalogue signifies that this said business has been subsumed under the ambit of the telecommunications licensing regime. Hence, an entity operating in this sector would need to apply for a license from the competent authority.

Since the new edition of the Catalogue came into effect, cloud service providers have progressively applied for qualification status with the relevant authorities. Tencent Cloud was granted the said CDN qualification in March 2017.

C5

Last updated : 2020-10-19 11:18:18

Tencent Cloud has passed the German C5:2020 basic and additional audit criteria, demonstrating that the security controls of Tencent Cloud services comply with the standards of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and can further meet the data security compliance requirements of Germany and Europe.

On August 31, 2020, Tencent Cloud passed the German BSI C5:2020 cloud security basic and additional audit criteria, proving its global leading position in the development of security policies and technical applications for cloud platforms. The Cloud Computing Compliance Criteria Catalogue (C5) was developed by the German BSI with the aim of verifying the information security compliance of cloud providers based on standardized inspections and reports.

The C5:2020 criteria include 17 objectives regarding the information security of cloud services, such as information security organization, security policies and instructions, personnel, asset management, and physical security, and stipulate general principles, procedures, and measures to achieve these objectives. Compared with the 2016 version, C5:2020 expands the criteria to add a new section “Dealing with investigation requests from government agencies" based on the EU Cybersecurity Act, which puts forward more stringent requirements for the security management levels of cloud providers.

C5:2020 is not only an essential cloud security benchmark for the adoption of cloud solutions by German government agencies and organizations, but it is also widely adopted by the private sector in Europe and around the world. Moreover, it is a high-level security standard recognized by the cloud industry and an important baseline for cloud providers to comply with the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) and the EU General Data Protection Regulation (GDPR).

Tencent Cloud's alignment with the C5:2020 basic and additional audit criteria demonstrates that its users are in strict compliance with German data security guidelines. This certification also enables Tencent Cloud to help users fully understand its security controls through a transparent communication mechanism, enhancing user trust in its services and products.