HUAWEI CLOUD Compliance with MPA – Application and Cloud Distributed Environment Security Guidelines

Issue 1.1

Date 2022-05-23

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

1.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and all its products and services available in HUAWEI CLOUD International website.

1.2 Purpose of Publication

Motion Picture Association, Inc. (MPA) is a leading advocate of the film, television and streaming industry around the world. Its members include Paramount Pictures, Inc., Sony Pictures Entertainment Inc., Universal City Studios LLC, Netflix, The Walt Disney Company and Warner Bros. Entertainment Inc. It has established a set of best practice standards for the securely storing, processing and delivering protected media and content, including *Content Security Best Practices- Common Guidelines* and *Content Security Best Practices- Application and Cloud/Distributed Environment Secruity Guidelines.*

In order to meet MPA's expectations on content security and current industry best practices, HUAWEI CLOUD conducted a self-assessment on the control requirements in various domains of *Content Security Best Practices- Application And Cloud/Distributed Environment Secruity Guidelines* in this document, showing customers the efforts made by HUAWEI CLOUD to improve content security and help customers understand:

- Main control requirements of *Content Security Best Practices- Application And Cloud/Distributed Environment Secruity Guidelines* in various domains;
- HUAWEI CLOUD's responses to the control requirements in various domains.

1.3 Basic Definitions

- **Customer (Tenant)**

  Refers to the registered users who build business relationships with HUAWEI CLOUD. In this whitepaper, customers has the same meaning of tenant which indicates the user organization that use the services provided by HUAWEI CLOUD.

- **Information Systems Audit and Control Association**

  Information Systems Audit and Control Association (ISACA) is a globally recognized leading organization for information technology governance, monitoring, security, and standards compliance.

- **System Administration Networking and Security Institute**

  System Administration Networking and Security Institute (SANS) is the most trusted and by far the largest source for information security training and security certification in the world. SANS provides intensive, immersion training designed to help the enterprise and its staff master the practical steps necessary for defending systems and networks against the most dangerous threats.

- **Cloud Security Alliance**

  The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

- **ISO 27001 Information Security Management System**

  ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls. ISO 27002 is the best practices based on ISO 27001.

- **ISO 27002 Practice Specification of Information Security Management**

  ISO 27002 is the best practice based on ISO 27001 and is also the official mapping standard of MPA general guidelines. The standard is established according to various guidelines and principles, and is used to initiate, implement, improve and maintain information security management within the organization.

- **ISO 27017 Cloud Service Information Security Management System**

  ISO 27017 is the practical rules for cloud service information security control based on the ISO 27001 system framework and ISO 27002 best practices. It is an international implementation procedures standard for cloud service information security control.

- **ISO 27018 Public Cloud Personal Identifiable Information (PII) Management System**

  Based on ISO / IEC Information Security Standard ISO 27002, ISO 27018 provides guidance on the implementation of control measures for personal information in public cloud. It aims to supplement the protection requirements of personal identifiable information (PII) in public cloud that the existing control system combination of ISO 27002 fails to meet.

- **ISO 22301 Business Continuity Management System**

  ISO 22301 is an international standard for business continuity management systems. ISO 22301 help organizations avoid potential incidents through identifying, analyzing and warning of risk, and formulate a complete business continuity plan to effectively respond to quick recovery after interruption and maintain normal running of core functions and minimize loss and recovery costs.

- **CSA CCM Cloud Security Alliance Cloud Control Matrix**

The world’s only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations.

- **SOC Audit Reports**

  The SOC audit reports are independent audit reports designed by a third-party audit institution based on relevant standards formulated by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.

- **PCI DSS Certification**

  Payment Card Industry Data Security Standard (PCI DSS) is a data security standard published by Payment Card Industry Security Standards Council which established by the five main credit card organizations: JCB, American Express, Discover, MasterCard, and Visa. For the content of HUAWEI CLOUD's PCI DSS certification, please refer to *HUAWEI CLOUD Practical Guide for PCI DSS*.

- **NIST Cybersecurity Framework**

  The NIST cyber security framework consists of three parts: standards, guidelines, and best practices for managing cyber security risks. The core content of the framework can be summarized as the classic IPDRR capability model namely the five capabilities: Identify, Protect, Detect, Response and Recovery.

- **Open Web Application Security Project**

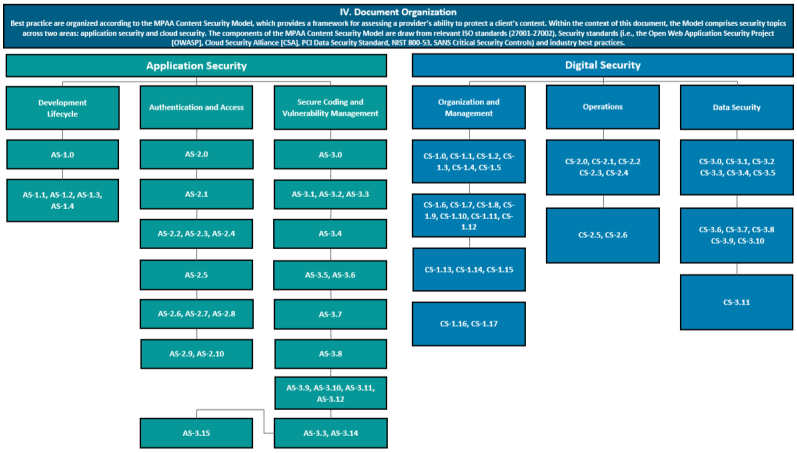
  Open Web Application Security Project (OWASP) is an online community dedicated to web application security. The OWASP community includes corporations, educational organizations and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools and technologies.

2 MPA Introduction

The Motion Picture Association (Hereinafter referred to as MPA) has been in existence for more than 30 years. Originally named after the Motion Picture Association of America (Hereinafter referred to as MPAA), Inc., the association changed its name in September 2019 to The Motion Picture Association, Inc. (MPA). MPA has established a set of best practice standards for the securely storing, processing and delivering protected media and content.

MPA best practices include *Content Security Best Practices-Common Guidelines* and *Content Security Best Practices-Application and Cloud Distributed Environment Security Guidelines*, which describe best practice control guidelines and implementation steps, taking into account relevant ISO standards, security standards, and industry best practices.

The Application and Cloud Distributed Environment Security Guidelines consists of 2 modules, 6 security topics and 69 controls. Its reference standards include ISO 27001, ISO 27002, OWASP, CSA, PCI DSS, NIST 800-54 and SANS.



In this document, HUAWEI CLOUD conducts self-assessment on *Content Security Best Practices-Application and Cloud Distributed Environment Security Guidelines* to meet the content security requirements of MPA, and improve the management and control ability of HUAWEI CLOUD in the fields of Management System, Physical Security, Digital Content Security, etc.

3 HUAWEI CLOUD MPA Evaluation Form - Content Security Best Practices - Application And Cloud/Distributed Environment Security Guidlines (v1.0)

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.0	SDLC	Build security into the entire Systems/ Software Development Lifecycle (SDLC).	By leveraging HUAWEI's wealth of experience and far-reaching capabilities in the field of security, HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also	12.5 14.1	12.5 14	12.5 14	SOC1 6.1 SOC1 6.3 SOC1 6.4 SOC1 6.5 SOC1 6.6	AIS-01 AIS-02 AIS-03 AIS-04 BCR-01 CCC-03	6.1 6.2 6.3 6.4 6.5 6.6	SA-3 SA-4 SA-8 SA-11 SA-12

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			seamlessly integrated the HUAWEI security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.1	SDLC	Test security across the entire application and infrastructure.	All cloud services pass multiple security tests before release. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. See *HUAWEI CLOUD Security White Paper* for details. In addition, HUAWEI CLOUD leverages its in-depth understanding of customers' security requirements and industry standards and develops matching security test tools. One such tool is SecureCAT, which can be used to							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			check security configurations of mainstream OS and database systems.							
AS-1.2	SDLC	Perform fuzz testing and defect remediation to discover security loopholes in software, operating systems or networks by massive inputting of random data to the system in an attempt to make it crash (e.g., buffer overflow, cross-site scripting, denial of service attacks, format bugs, SQL injection).	HUAWEI CLOUD has established an attack mode database, which is tested through attack mode library in the cloud service test phase. The attack mode library includes buffer overflow, cross site script, denial of service attack, format error, SQL attack and other attack modes.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.3	SDLC	Perform bug tracking and defect remediation in conjunction with extensive black box testing, beta testing, and other proven debugging methods.	All cloud services pass multiple security tests before release. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. See HUAWEI CLOUD Security White Paper for more details.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.4	SDLC	Provide training and user guides on additions and changes to the application.	After the application is changed, HUAWEI CLOUD will update the user guide on the official website. Customers can contact HUAWEI CLOUD customer service for corresponding support if they have any questions during the use.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.0	Authentication and Access	Implement secure authentication.	The access control capabilities of HUAWEI CLOUD are facilitated through its Identity and Access Management (IAM) service. The IAM service is a security management service optimized for enterprise tenants. Through the IAM service, tenants can manage users and security credentials (such as access keys) in a centralized manner and control users' administrative privileges and cloud resource access permissions. See *HUAWEI CLOUD Security White Paper* for more details.	9.1 9.2 9.3 9.4	9.1 9.2 9.3 9.4	9.1 9.2 9.3 9.4	SOC1 2.1 SOC1 2.2 SOC1 2.3 SOC1 2.4 SOC1 2.5 SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8	IAM-01 IAM-02 IAM-03 IAM-04 IAM-05 IAM-06 IAM-07 IAM-08 IAM-09 IAM-10 IAN-11 IAM-12 EKM-02 EKM-04 IVS-01	7.1 8.1 8.2	AC-2 AC-3 AC-6 AC-7 AC-8 AC-14 IA-5 IA-6 IA-8

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.1	Authentication and Access	Register user devices.	All O&M, device, and application accounts are centrally managed. All accounts are centrally monitored and automatically audited through the unified audit platform. Therefore, the entire account lifecycle is well managed, from account creation, permissions granting, permissions verification and access granting, and account and permissions deletion.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.2	Authentication and Access	Implement secure password recovery.	HUAWEI CLOUD provides customers with Data Encryption Workshop (DEW) supports key escrow, which can help customers easily create and manage keys. Based on DEW, customers can realize the full life cycle management of keys.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.3	Authentication and Access	Follow the principle of least privilege.	HUAWEI CLOUD has different responsibilities according to different business roles, access permissions management applies RBAC and includes the following basic roles: core network, access network, security devices, service systems, database systems, hardware maintenance, and monitoring maintenance. Any O&M personnel is restricted to access only devices within the administrative scope of his/her role and is not granted permissions to access other devices.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.4	Authentication and Access	Implement controls to prevent brute force attacks.	Identity Access Management (IAM) supports setting account locking policy, account deactivation policy and session timeout policy that meet customer requirements. After the account locking policy is set, the failed login account will be locked after the number of login failures reaches the set value within a limited time, and the number of times can be set between 3 and 10. IAM supports inactive days of 1~240 days. If an account is not							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			registered within days of setup, it will be discontinued. If the session does not operate within the set duration, you need to log in again.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.5	Authentication and Access	Implement and document a process to secure key / cryptographic storage and ensure ongoing secure management.	HUAWEI CLOUD provides customers with data encryption service Data Encryption Workshop (DEW), which can provide exclusive encryption, key management, key pair management and other functions. All the keys in Key Management Service (KMS) are generated by the hardware true random number generator of HSM to ensure the randomness of the key. Key disclosure is prevented by storing the root key of the KMS in the HSM. The root key at no time appears outside the							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			HSM. KMS hosts use standard encrypted transmission mode to establish secure communication links with KMS service nodes to ensure the transmission security of KMS related data between nodes. KMS implements RBAC access control based on IAM role. All operations on the key (such as creating user master key, encrypting data key, etc.) will generate logs and record them to the Cloud Audit Service (CTS) for later audit.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.6	Authentication and Access	Enable an auto-expiration setting to expire all external links to content after a user-defined time.	If the session does not operate within the set duration range, customers need to log in again. Identity Access Management (IAM) supports a minimum of 15 minutes of session timeout.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.7	Authentication and Access	Use human verification tools such as CAPTCHA or reCAPTCHA with web applications.	HUAWEI CLOUD provides users with cloud web application firewall service (WAF), which can be based on IP, cookie and referer information are used to identify users, and flexibly configure the threshold to implement the access speed limit. For the visitors who exceed the threshold, their requests can be blocked to avoid the pressure on the business; verification code challenge can also be launched for human-computer identification, so that the attackers can be more							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			accurately identified and blocked.							
AS-2.8	Authentication and Access	Provide clients with the ability to limit the number of times an asset may be downloaded or streamed by a particular user.	In some services of HUAWEI CLOUD, customers' permissions to a file (such as browsing, downloading, editing, etc.) can be restricted, as well as the validity period of permissions.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.9	Authentication and Access	Confirm the upload and download of all content and critical assets.	HUAWEI CLOUD has a centralized and complete logs big data analysis system. The system uniformly collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems, as well as threat detection alarm logs of various security products and components.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.10	Authentication and Access	Include a brief message on mobile applications to remind users to enable device passwords and to enable remote wipe and device location software.	Mobile devices can access the enterprise office environment of HUAWEI CLOUD through the internal application required by work, such as timely communication, emails, forums, human management, etc., for which corresponding rules and regulations have been established. However, HUAWEI CLOUD does not support mobile devices such as IOS or Android phones and tablets to access the production environment, especially customer content data.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.0	Security Coding and System	Perform penetration testing / web application security testing prior to production deployment, and at least quarterly thereafter. Validate vulnerabilities were remediated with a retest.	All cloud services pass multiple security tests before release. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. See *HUAWEI CLOUD Security White Paper* for more details. HUAWEI CLOUD will organize internal and external qualified third parties to scan all systems, applications and networks of HUAWEI CLOUD every quarter. It also employs an external third party to conduct	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	SOC1 3.4 SOC1 3.6 SOC1 10.4	STA-05 STA-09 AIS-03 IVS-01 SEF-02 SEF-05 DSI-03	1.2 1.3 1.4 5.1 5.2 5.3 10.6 11.1 11.2 11.3	AC-18 AU-5 CA-3 CA-9 SC-15 SC-18 SC-19 SC-32 SC-7 SI-10 SI-11 SI-2 SI-3 SI-4 SI-8

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			penetration tests on HUAWEI's Cloud Applications and networks every six months.							
AS-3.1	Security Coding and System	Perform vulnerability testing at least quarterly.	HUAWEI CLOUD will organize internal and external qualified third parties to scan all systems, applications and networks of HUAWEI CLOUD every quarter. It also employs an external third party to conduct penetration tests on HUAWEI's Cloud Applications and networks every six months.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.2	Security Coding and System	Utilize cookies in a secure manner (if they need to be used).	HUAWEI CLOUD formulates cookie policy that adapts to local requirements, and deploys web application firewall to deal with web attacks, including cookie injection of attack mode library, to protect web application services and systems deployed in DMZ area and facing external network.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.3	Security Coding and System	Validate user input and implement secure error handling.	According to integrity control described in the SOC report, HUAWEI CLOUD has formulated policies and procedures for maintaining data integrity control in all stages of the data life cycle (including transmission, storage, and processing), and regularly relies on internal and external audits to verify their effectiveness. For the integrity verification of the content data, the customer is responsible for the implementation of input and output verification							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			control in the application interfaces and databases used in the HUAWEI CLOUD environment.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.4	Security Coding and System	Implement secure logging procedures.	HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses,							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			host IDs, and user IDs), event types, date and time, IDs of the affected data/ components /resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.5	Security Coding and System	Implement an SIEM (Security Information Event Management System) to aggregate and analyze the disparate logs.	HUAWEI CLOUD uses CLS log system to monitor system components, collect, store and analyze all system component logs, and independently developed CIP centralized security event management system to analyze security events and give real-time alarms. The system conducts intelligent analysis based on threat model and expert defined rules. HUAWEI CLOUD will also review the log and the handling of security incidents on a regular basis. HUAWEI CLOUD							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			monitors the key infrastructure and network, which can timely monitor possible network attacks and avoid data leakage events. HUAWEI CLOUD has established a response process for network security incidents. Multiple departments cooperate to monitor the incident in time, and quickly deploy disposal measures to reduce the impact of the incident.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.6	Security Coding and System	Encrypt all content and client data at rest.	Customers have the ownership and control of the content data, and are responsible for the quality of their content data and bear the risk caused by the data quality. HUAWEI CLOUD uses the key management system to encrypt and manage the encryption key. The strength of data encryption key (DEK) and key encryption key (KEK) are AES strong encryption algorithms. Several services of HUAWEI CLOUD are integrated with key management service (DEW),							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			which is convenient for customers to manage key. Customers can store and encrypt data through simple encryption settings.							
AS-3.7	Security Coding and System	Encrypt all content and client data in transit.	In the process of network transmission, HUAWEI CLOUD uses TLS high version secure transport layer protocol and IPSec protocol, and uses secure transmission channel or AES strong encryption algorithm to strictly encrypt sensitive data between untrusted networks.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.8	Security Coding and System	Implement controls for secure session management.	HUAWEI CLOUD refers to the solution of session security design in the industry, aiming at the common vulnerabilities and potential risks in session management, and combining with the current situation of the company, designs and implements management control mechanisms such as session generation, maintenance and destruction.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.9	Security Coding and System	Implement controls to prevent SQL injection.	When developing services, HUAWEI CLOUD will consider all kinds of possible attacks, and design and develop corresponding controls. In the cloud service testing stage, the attack pattern library should be tested. The attack pattern library includes buffer overflow, cross site scripting, denial of service attack, format error, SQL attack and other attack patterns.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.10	Security Coding and System	Implement controls to prevent unvalidated URL redirects and forwards.	When developing services, HUAWEI CLOUD will consider all kinds of possible attacks, and design and develop corresponding controls. In the cloud service testing stage, the attack pattern library should be tested. The attack pattern library includes buffer overflow, cross site scripting, denial of service attack, format error, SQL attack and other attack patterns.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.11	Security Coding and System	Implement controls to prevent connections from anonymity networks (e.g., Tor, Freenet, Netshade), if possible.	When developing services, HUAWEI CLOUD will consider all kinds of possible attacks, and design and develop corresponding controls. In the cloud service testing stage, the attack pattern library should be tested. The attack pattern library includes buffer overflow, cross site scripting, denial of service attack, format error, SQL attack and other attack patterns.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.12	Security Coding and System	Implement controls to prevent IP address leakage.	When developing services, HUAWEI CLOUD will consider all kinds of possible attacks, and design and develop corresponding controls. In the cloud service testing stage, the attack pattern library should be tested. The attack pattern library includes buffer overflow, cross site scripting, denial of service attack, format error, SQL attack and other attack patterns.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.13	Security Coding and System	Implement controls to prevent XSS (Cross-site scripting).	When developing services, HUAWEI CLOUD will consider all kinds of possible attacks, and design and develop corresponding controls. In the cloud service testing stage, the attack pattern library should be tested. The attack pattern library includes buffer overflow, cross site scripting, denial of service attack, format error, SQL attack and other attack patterns.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.14	Security Coding and System	Allow senders the option to include session-based forensic (invisible) watermarking for content.	HUAWEI CLOUD will not check the quality of the content data of customers. HUAWEI CLOUD maintains quality management and risk control measures of customer personal data. For details, please refer to the **HUAWEI CLOUD Data Security White Paper**. Customers have ownership and control over the content data, are responsible for the quality of the content data and bear the risks associated with the quality of the data.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.15	Security Coding and System	Implement a formal, documented content / asset lifecycle.	HUAWEI CLOUD builds the security protection capability of full data life cycle. Through the research and application of automatic sensitive data discovery, dynamic data desensitization, high-performance and low-cost data encryption, rapid abnormal operation audit, data security destruction and other technologies, the management and control of data in the creation, storage, use, sharing, archiving, destruction and other links are realized to ensure the data security							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			on the cloud.							
CS-1.0	Organization and Management	Compliance with the MPA Content Best Practices Common Guidelines is required. Where stronger controls exist within the Application Security and Cloud/ Distributed Environment Guidelines, the stronger policy will prevail.	HUAWEI CLOUD has conducted a self-assessment on the requirements of general guidelines for MPa content best practices. For details, please refer to 3.1 of this document for details.	5.1 6.1	5.1 6.1 7 8.2 10.1 12.1 15.1 16.1 CLD.8.1	5.1 6.1 7 8.2 10.1 12.1 15.1 16.1 A.4.1 A.9.1 A.9.3 A.10.1 A.10.7 A.10.12 A.10.13 A.11.1	SOC1 1.1 SOC1 1.2 SOC2 9.3 SOC2 9.4 SOC2 9.8 SOC2 10.1 SOC2 10.3 SOC2 10.4	GRM-03 AAC-01 AAC-02 GRM-01 HRS-03 STA-05 DSI-02 AIS-02 AIS-03 AIS-04 DSI-01 DSI-07 BCR-01 BCR-11 PCI-12 EKM-03 IAM-02 STA-07	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7 7.3 8.1 8.4 8.8 9.10 10.8 11.6 12.1 12.3 12.4	AC-1 AC-18 AC-19 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SC-1 SI-1

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.1	Organization and Management	Perform a third party security audit at least once per year (e.g., SSAE 16 Type 2, SOC 1, ISO 27000/27001, MPA).	HUAWEI CLOUD has passed the audit of data security, privacy and security by an independent third party and obtained certification. The relevant certifications include: ISO27001, ISO27017, ISO27018, CSA STAR, ISO27701, ISO29151, SOC1 / SOC2 / SOC3, PCI DSS. Relevant certificates or reports can be obtained from **the trust center compliance**. HUAWEI CLOUD will invite a third party to review the above standards every year.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.2	Organization and Management	Document and implement security and privacy policies that are aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO-22307, CoBIT).	According to the requirements of ISO27001, ISO27701 and other standards, HUAWEI CLOUD must issue and implement corresponding security and privacy policies. Every year, HUAWEI CLOUD will invite a third party to review the effectiveness and implementation of security and privacy policies.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.3	Organization and Management	Document and implement information security baselines for every component of the infrastructure (e.g., Hypervisors, operating systems, routers, DNS servers, etc.).	HUAWEI CLOUD leverages the Minimum Security Baselines set out by the Center of Internet Security (CIS) and has integrated them into the HUAWEI CLOUD DevSecOps process. CIS security baselines are a set of industry best practices for cyber and system security configurations and operations, which cover people (behavior of both end users and administration personnel), processes (network and system management) and technologies (software							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			and hardware). HUAWEI CLOUD establishes an internal technical standard specification library, which contains the information security baselines for every component in the infrastructure.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.4	Organization and Management	Document and implement personnel security procedures that align with the organization's current information security procedures.	ISO27001 information security management system requires enterprises to publish and implement personnel security procedures that conform to the current information security procedures of the organization. HUAWEI CLOUD has obtained ISO27001 information security management system certification, and invites a third-party audit organization to audit every year.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.5	Organization and Management	Require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the onboarding process.	Newly hired or experienced employees of HUAWEI CLOUD must first sign employment contracts and confidentiality agreements, and complete information security relevant trainings before granting employees users access right to company facilities, resources, and assets. Supplier security and privacy requirements are included in the signed contract agreement. Business personnel docking with third parties are responsible for managing							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			their third-party relationships, including asset protection requirements and supplier access to related applications.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.6	Organization and Management	Document and implement procedures for conducting security due diligence when offloading functionality or services to a third party.	HUAWEI CLOUD has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation after to manage the supplier's compliance with the specific requirements and contract obligations of HUAWEI CLOUD. HUAWEI CLOUD's legal team will also regularly review the terms of the contract.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.7	Organization and Management	Document and implement segregation of duties for business critical tasks.	Based on different business roles and responsibilities, access permissions management applies RBAC and includes the following basic roles: core network, access network, security devices, service systems, database systems, hardware maintenance, and monitoring maintenance. Any O&M personnel is restricted to access only devices within the administrative scope of his/her role and is not granted permissions to access other devices.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.8	Organization and Management	Provide clients with information regarding locations for their content and data.	Customers can select and determine the specific geographic location of the content data store when they first configure the service. HUAWEI CLOUD will not move customer content from selected regions without notifying customers, unless it is necessary to comply with the requirements of laws or government entities.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.9	Organization and Management	Develop a documented procedure for responding to requests for client data from governments or third parties.	HUAWEI CLOUD would sign the **HUAWEI CLOUD Customer Agreement**, **Privacy Statement**, **Acceptable Use Policy**, *Service Statement and* **Service Level Statement** with customers before providing services. These agreements outline the service requirements and the responsibilities of both parties. For the client data requirements proposed by the government or the third party, HUAWEI CLOUD will provide them according to the local laws and							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			regulations and the agreement with customers. For more details, please refer to **HUAWEI CLOUD Security White Paper**.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.10	Organization and Management	Establish policies and procedures for labeling, handling, and securing containers that contain data and other containers.	ISO 27001 standard requires the identification of information security assets. HUAWEI CLOUD has passed the ISO 27001 certification, and has established a list and corresponding management procedures for its information security assets. Customers are the owners and controllers of their content data. Customers should establish corresponding control strategies for the label and processing of their content data to ensure the data security.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.11	Organization and Management	Establish procedures for the secure deletion of content/ data, including archived and backed-up content/ data.	HUAWEI CLOUD supports the secure deletion according to customer requirements. The secure deletion methods include deleting the encrypted storage encryption key, recycling and overwriting the underlying storage, and degaussing/ bending/ shredding the scrapped physical medium.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.12	Organization and Management	Establish, document and implement scenarios to clients in which client content/ data may be moved from one physical location to another.	HUAWEI CLOUD has obtained the certification of the ISO22301 business continuity management system standard, establishing a business continuity management system internally, and formulating a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.13	Organization and Management	Establish, document and implement additional key management features, controls, policies and procedures.	ISO27001 stipulates that enterprises should establish and implement policies and procedures for key management. HUAWEI CLOUD has established an encryption strategy and key management mechanism to protect data on technical equipment, including the assignment of personnel rights and responsibilities, encryption levels, and encryption methods. Data Encryption Workshop (DEW) provided by HUAWEI CLOUD supports key escrow,							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			which can help customers easily create and manage keys. Based on DEW, customers can realize the full life cycle management of keys and record the ownership of keys.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.14	Organization and Management	Train personnel regarding all policies and procedures.	To raise cybersecurity awareness company wide, avoid non compliance risks, and ensure normal business operations, Huawei provides employee security awareness training in three ways: company wide awareness training, awareness promotion events, and the signing of BCG commitment agreements. . For more details, please refer to *HUAWEL CLOUD Security White Paper*.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.15	Organization and Management	Establish a process to notify clients when material changes are made to security/ privacy policies.	To protect end users and tenants, HUAWEI CLOUD upholds the principle of responsible disclosure. While ensuring no undue risks of potential exploitation and attacks will result from the disclosure of any vulnerability, HUAWEI CLOUD continues to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and customers vulnerability mitigation solutions, standing shoulder to shoulder with our customers in tackling							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			security challenges caused by endless vulnerabilities.							
CS-1.16	Organization and Management	Plan, prepare and measure the required system performance to ensure acceptable service levels.	HUAWEI CLOUD provides customers with the content of the SLA agreement on the official website. Customers can refer to the HUAWEI CLOUD **Service Level Agreement** page for more information.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.17	Organization and Management	Develop and maintain additional requirements for incident response and immediate notification to the client in the event of any unauthorized access to systems or content.	HUAWEI CLOUD establishes a response process to respond to cyber security incidents, and monitors critical infrastructure and networks, which can detect possible cyber-attacks in time and avoid data leakage incidents. In areas where HUAWEI CLOUD operates, if a data breach occurs, a dedicated person is responsible for notifying customers and local regulatory authorities.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.0	Operation	Secure datacenter utilities services and environmental conditions.	The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers, including power supply, temperature and humidity control, fire fighting capability, routine monitoring, water supply and drainage, etc. For details, please refer to *HUAWEI CLOUD*	11.1 11.2 11.5	8.1 11.1 12.1	8.1 11.1 12.1	SOC1 5.1 SOC1 5.3 SOC1 5.4 SOC1 5.5 SOC1 5.6 SOC1 5.7 SOC1 5.8 SOC1 5.9 SOC1 5.10 SOC1 5.11 SOC1 5.12 SOC1 10.4	DCS-01 DCS-02 DCS-03 DCS-04 DCS-05 DCS-06 DCS-07 DCS-08 DCS-09 BCR-01 BCR-02 BCR-03 BCR-06 GRM-06	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7 7.3 8.1 8.4 8.8 9.2 9.4 9.10 10.8 11.6 12.1 12.3	PE-1 PE-18 PE-2 PE-3 PE-4 PE-5 PE-6 PE-8 PE-9 PL-8 PS-1

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			Security White Paper.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.1	Operation	Ensure the data center has appropriate perimeter and physical security controls.	HUAWEI CLOUD data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. Security guards routinely patrol data centers and set up							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			online electronic patrol systems. For details, please refer to *HUAWEI CLOUD Security White Paper*.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.2	Operation	Develop, document and maintain additional requirements for business continuity planning.	HUAWEI CLOUD has obtained the certification of the ISO22301 business continuity management system standard, establishing a business continuity management system internally, and formulating a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies. For more details about business continuity, please refer to *HUAWEI CLOUD Security White Paper*.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.3	Operation	Develop, document and maintain additional change and configuration controls.	HUAWEI CLOUD has established the system change management and service launch process, and communicated its requirements to all relevant developers (including internal employees and external partners). The newly launched or changed services shall follow the regulations of HUAWEI CLOUD release and change management process.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.4	Operation	Maintain a complete inventory of all critical assets, including ownership of the asset.	According to the ISO27001 standard, HUAWEI CLOUD's information asset classification is monitored and managed by special tools to form an asset list, and each asset is assigned an owner. HUAWEI CLOUD has obtained ISO27001 certification, and the certification can be downloaded from the Trust Center.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.5	Operation	Maintain an inventory of all critical supplier relationships.	HUAWEI CLOUD has formulated supplier security management requirements, and regularly reviews suppliers to verify whether they meet HUAWEI CLOUD security and privacy standards.							
CS-2.6	Operation	Develop and maintain service level agreements (SLA's) with clients, partners, and service providers.	HUAWEI CLOUD provides customers with the content of the SLA agreement on the official website. Customers can refer to the HUAWEI CLOUD **Service Level Agreement** page for more information.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.0	Data Security	Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.	HUAWEI CLOUD provides customers with cloud audit service (CTS) which records operations performed on the management console, executed through an API, and internally triggered on the HUAWEI CLOUD system. For more details, please refer to *HUAWEI CLOUD Security White Paper*.	11.2 12.1	11.2 12.1 CLD. 9.5 CLD. 13.1	11.2 12.1 A. 10.13	SOC1 3.1 SOC1 3.2 SOC1 3.3 SOC1 3.5 SOC1 3.6 SOC1 3.9 SOC1 3.10 SOC1 3.11 SOC1 3.12 SOC1 3.13 SOC1 3.14 SOC1 3.15 SOC1 3.16 SOC1 7.1 SOC1 7.2 SOC1 7.3 SOC1 7.4 SOC1 7.5 SOC1 7.6 SOC1 7.7 SOC1 7.8	DSI-01 DSI-02 DSI-03 DSI-04 DSI-05 DSI-06 DSI-07	1.1 1.2 1.3 1.4 6.4 10.4 12.5	AC-3 AC-4 AC-5 AU-8 CA-3 CA-9 CM-6 CM-7 SC-19 SC-5 SC-7 SI-4

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.1	Data Security	Consider providing the capability to use system geographic location as an additional authentication factor.	HUAWEI CLOUD's Identity Access Management (IAM) is authorized according to the hierarchy and fine-grained authorization, and manages the user's rights through password authentication, multi factor authentication and Federation authentication.				SOC1 10.4			

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.2	Data Security	Provide the capability to control the physical location/ geography of storage of a client's content/ data, if requested.	Customers can select and determine the specific geographic location of the content data store when they first configure the service. HUAWEI CLOUD will not move customer content from selected regions without notifying customers, unless it is necessary to comply with the requirements of laws or government entities.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.3	Data Security	Establish procedures to ensure that non-production data must not be replicated to production environments.	HUAWEI CLOUD uses a combination of physical and logical control isolation methods for production and non-production environments, this combined isolation methods improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal incompliance.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.4	Data Security	Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/ data once the client contract has terminated.	In the destruction stage of customer content data, HUAWEI CLOUD will completely clear the specified data and all its copies. After the customer confirms the deletion of operation, HUAWEI CLOUD will first delete the index relationship between the customer and the data, and clear the operation before reallocating the memory, block storage and other storage space to ensure that the relevant data and information cannot be restored. For the scrapping of physical							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			storage media, HUAWEI CLOUD eliminates the data by degaussing, bending or breaking the storage media to ensure that the data on it cannot be recovered. HUAWEI CLOUD supports customers to cancel their accounts. When the customer applies for account cancellation and passes the account verification by HUAWEI CLOUD, the customer content data enters the retention period. During the retention period, the customer cannot access and use the cloud service, but							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			the data stored in the cloud service is still retained. After the expiration of the retention period, the customer content data will be completely cleared and cannot be restored.							
CS-3.5	Data Security	Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization ’s premises.	For the scrapped physical storage media, HUAWEI CLOUD eliminates the data by degaussing, bending or breaking the storage media to ensure that the data on it cannot be recovered.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.6	Data Security	Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.	HUAWEI CLOUD uses the NTP4.2.8 protocol to synchronize the time in the system.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.7	Data Security	Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.	According to the business function and network security risk, HUAWEI CLOUD divides the production network into DMZ area, public service area, resource delivery area, data storage area and operation and maintenance management area through physical and logical control. The resource delivery area provides the infrastructure resources required by customers, including computing, storage and network resources, such as customers' virtual machine, disk and virtual							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			network. The multi-layer security control means are used to realize resource isolation among tenants, and the tenants can not access the resources of other customers; the platform side management plane and data storage plane are isolated, and they are isolated from the tenant data plane. This area can also support DDoS protection and intrusion detection and defense for customer traffic in and out of the Internet, so as to guarantee the tenant business.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.8	Data Security	Design, develop and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented.	HUAWEI CLOUD carries many customers' data. Each service product and component has planned and implemented an isolation mechanism from the beginning of the design, to avoid intentional or unintentional unauthorized access tampering among customers, so as to reduce the risk of data leakage. HUAWEI CLOUD's isolation of cloud data is implemented through a virtual private cloud VPC, which uses network isolation technology to achieve complete							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			isolation between different tenants on the three-layer network.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.9	Data Security	Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/ from virtual servers.	The Cloud Data Migration Service (CDM) runs in the user's VPC, and network isolation ensures the security of data transmission. Data sources that support SSL, such as RDS, SFTP, etc., can use SSL. CDM also supports data from public network data sources to the cloud, and users can use VPN and SSL technology to avoid transmission security risks. The access information (user name and password) of the user data source is stored in the database of the CDM instance and							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			encrypted with AES-256.							
CS-3.10	Data Security	Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/ egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).	To improve the security of cloud services, HUAWEI CLOUD applies a variety of advanced protection functions to protect the intranet area, including DDoS anomaly and large traffic cleaning, Network intrusion detection and interception, Web security protection. See *HUAWEI CLOUD Security White Paper* for details.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.11	Data Security	Establish and document controls to secure virtualized environments.	HUAWEI CLOUD's Unified Virtualization Platform (UVP) abstracts physical server resources such as CPU, memory, and input/output (I/O) resources, and converts them into a pool of logical resources that can be centrally managed, flexibly scheduled, and dynamically assigned. Based on the logical resources, the UVP provisions a number of VM execution environments, which run concurrently but are isolated from each other, on a single physical server.							

NO.	Security Topic	Best Practice	HUAWEI CLOUD's Responses	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
			HUAWEI CLOUD's UVP OS has been awarded the highest rating Five Star Plus Certification as part of HUAWEI CLOUD's China DCA Trusted Cloud Certification.							

4 Conclusion

HUAWEI CLOUD always adheres to HUAWEI's "customer-centric" core values and actively implement information security practices resulting in the establishment of an information security management system, certification and audit of a third-party organization to check the effective implementation of security controls and the deployment of the most common data security protection technologies in the industry to protect customers data security.

Simultaneously, in order to help customers cope with the increasingly openness and complexity of network environments and the development of new information security technologies, HUAWEI CLOUD continuously develops various products, services and solutions in the field of data protection to support customers in improving their data protection ability and reducing their risks.

This white paper is for customers' reference only and does not have any legal effect or constitutes legal advice, nor does it serve as a basis for certain compliance of customers' cloud environment when using HUAWEI CLOUD. Customers should evaluate their own operation and security requirements, selecting appropriate cloud products and services.

5 Version History

Date	Version	Description
2022-4	1.1	Routine update
2021-1	1.0	First Publication

