HUAWEI CLOUD Compliance with CSA CCM (CSA CAIQ v3.1)

Issue 01

Date 2020-09-30

HUAWEI 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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

The Cloud Security Alliance Cloud Control Matrix (CSA CCM) published by the Cloud Security Alliance, as a controls framework for cloud security, integrates advanced standards, regulations and best practices to assist cloud providers and cloud customers in improving cloud security.

HUAWEI CLOUD has already gained the cloud security certification —— CSA STAR Gold Certification, and hope through the CAIQ self-assessment questionnaire in this material to show the customers that HUAWEI CLOUD's efforts to improve the security of cloud environment, and to help customers understand:

- CSA CCM's main contents, related certification and the function of CAIQ;
- HUAWEI CLOUD's responses to questions in CAIQ self-assessment questionnaire.

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.

- **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.

- **British Standards Institution (BSI)**

  An internationally renowned standard certification organization providing standard certification and training services for organizations and individuals worldwide.

- **CSA CCM**

  Cloud Security Alliance Cloud Control Matrix is the world's only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations.

- **CSA CAIQ**

  The Consensus Assessments Initiative Questionnaire (CAIQ) v3.1 offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency. It provides a set of Yes/No questions a cloud customer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM).

- **CSA STAR Certification**

  An authoritative certification for cloud security level launched by the CSA and the BSI together, where STAR is the abbreviation for Security, Trust, Assurance and Risk. The certification is evaluated and audited based on the requirements of CSA CCM and ISO 27001.

- **ISO27001 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 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 27701 Privacy Information Management System**

  As a privacy extension to ISO 27001 and ISO 27002, ISO 27701 is an authoritative international standard of privacy management field. ISO 27701 specifies requirements and guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS) and its relevant content.

- **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.

- **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*.

- **PCI 3DS Certification**

  The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. The evaluation object of PCI 3DS is the 3D protocol execution environment, including the access control server, directory server, or 3DS server functions; And system components, such as firewalls, virtual servers, network devices, and applications, that are within and connected to the 3D execution environment; In addition, the process, process, and personnel management of the 3D protocol execution environment will be evaluated.

- **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.

- **M&O certification**

  Uptime Institute is a globally recognized data center standardization organization and an authoritative professional certification organization. HUAWEI CLOUD data centers have obtained the M&O certification issued by Uptime Institute. The M&O certification symbolizes that HUAWEI CLOUD data center O&M management has been leading in the world.

2 CSA CCM Introduction

2.1 CSA CCM Framework and Main Content

CSA CCM is a cloud security guide issued by the Cloud Security Alliance, a leading international cloud security organization. Cloud security Alliance was established in 2009, committed to the comprehensive development of international cloud computing security. At present, the Cloud Security Alliance has assisted the governments of the United States, the European Union, Japan, Australia, Singapore and other countries to carry out national network security strategy, national identity strategy, and national cloud computing strategy, national cloud security standards, government cloud security framework, security technology research and other work.

CCM includes Control Domains, Control Specification, Architectural Relevance corresponding to each Control Specification, Corporate Governance Relevance, and types of Cloud Service Delivery Model, relevance to Service Provider and Customers and mapping to 42 standards, regulations, and best practices. As shown in the figure below, CCM composed of 133 control specifications that are structured in 16 domains covering common control measures related to cloud security.

Control ID	Control Domain
AIS	1. Application & Interface Security
AAC	2. Audit Assurance & Compliance
BCR	3. Business Continuity Management & Operational Resilience
CCC	4. Change Control & Configuration Management
DSI	5. Data Security & Information Lifecycle Management
DCS	6. Datacenter Security
EKM	7. Encryption & Key Management
GRM	8. Governance and Risk Management

Control ID	Control Domain
HRS	9. Human Resources
IAM	10. Identity & Access Management
IVS	11. Infrastructure & Virtualization Security
IPY	12. Interoperability & Portability
MOS	13. Mobile Security
SEF	14. Security Incident Management, E-Discovery, & Cloud Forensics
STA	15. Supply Chain Management, Transparency, and Accountability
TVM	16. Threat and Vulnerability Management

2.2 CSA, CCM, CAIQ, and STAR Certification

The cloud security control consists of independent assessment of external third parties and internal continuous management of cloud service providers.

Based on CCM and ISO 27001, the Cloud Security Alliance (CSA) and the British Standards Institute (BSI) have jointly developed the CSA STAR Certification. By evaluating cloud service providers, and certifying and rating the cloud service provider into 3 grades of gold, silver or bronze by the implementation of control measures required by CCM and ISO 27001, and the rating results have three grades: gold, silver or bronze.

According to CSA CCM, the Cloud Security Alliance has launched CAIQ Consensus Assessment Initiative Questionnaire for cloud service providers to assess their control levels. The control domains and control specification of the questionnaire were consistent with CCM, but each control specification is subdivided into multiple answerable questions, in total, 330 questions. Cloud service providers can use CAIQ for self-assessment and use CAIQ to continuously manage their own control levels.

Presenting HUAWEI CLOUD's response to CAIQ, Chapter 3 of this material will help customers understand HUAWEI CLOUD's efforts to strengthen its own cloud security level and improve security in the cloud. The CAIQ used in this material is the latest version 3.1 released in 2020.

2.3 The Certification Status of HUAWEI CLOUD

With its own information security system and security control management, HUAWEI CLOUD has obtained the highest level of CSA STAR certification - CSA STAR Gold Certification. The assessment scope includes dozens of products and services released by HUAWEI CLOUD on its official website, as well as data centers around the world.

HUAWEI CLOUD products and services covered by the 2020 STAR certification are as follows (refer to HUAWEI CLOUD official website for specific online areas), and HUAWEI CLOUD's CSA STAR certificate can be download from the HUAWEI CLOUD Trust Center for reference.

Categories	Products
Compute	Elastic Cloud Server (ECS), Bare Metal Server (BMS), CloudPhone (CPH), Dedicated Host (DeH), Auto Scaling (AS), Image Management Service (IMS), GPU Accelerated Cloud Server (GACS), and FPGA Accelerated Cloud Server (FACS)
Storage	Object Storage Service (OBS), Elastic Volume Service (EVS), Cloud Backup and Recovery (CBR), Dedicated Enterprise Storage Service (DESS), Dedicated Distributed Storage Service (DSS), Volume Backup Service (VBS), Cloud Server Backup Service (CSBS), Storage Disaster Recovery Service (SDRS), Scalable File Service (SFS), Data Express Service (DES), and Cloud Storage Gateway (CSG)
Networking	Virtual Private Cloud (VPC), Elastic Load Balance (ELB), NAT Gateway (NAT), Elastic IP (EIP), Direct Connect (DC), Virtual Private Network (VPN), Cloud Connect (CC), and VPC Endpoint (VPCEP)
Database	Document Database Service (DDS), Distributed Database Middleware (DDM), Data Admin Service (DAS), Distributed Database Middleware (DRS), RDS for MySQL (MySQL), RDS for PostgreSQL (PostgreSQL), RDS for SQL Server (SQL Server), RDS for GaussDB (for MySQL) (GaussDB for MySQL), and RDS for GeminiDB (GeminiDB)
Container Service	Cloud Container Engine (CCE) and Cloud Container Instance (CCI)
Video	Live (Live), Video on Demand (VOD), Media Processing Center (MPC), and Short Video (SVideo)
Application Middleware	Distributed Cache Service Redis (DCS), Distributed Cache Service Memcached (DCSMEM), Distributed Message Service DMS (DMS), Distributed Message Service (Kafka), Distributed Message Service RabbitMQ (RabbitMQ), API Gateway (APIG), and application management and O&M platform (ServiceStage)
Management Tools	Application Operations Management (AOM), Application Performance Management (APM), Log Tank Service (LTS), Identity and Access Management (IAM), Cloud Eye (CES), Simple Message Notification (SMN), and Cloud Trace Service (CTS)
Domains and Websites	Domain Name (Domains), Cloudsite, and Domain Name Service (DNS)
Migration	Object Storage Migration Service (OMS) and Cloud Data Migration (CDM)

Categories	Products
Intelligent Cloud Acceleration	Content Delivery Network (CDN)
Software Developmen t Platform	CodeHub, CodeCheck , CloudBuild, ProjectMan, and CloudIDE
Security	Host Security Service (HSS), Container Guard Service (CGS), Web Application Firewall (WAF), Vulnerability Scan Service (VSS), Anti-DDos (Anti-DDos), Advanced Anti-DDoS (AAD), Database Security Service (DBSS), Data Encryption Workshop (DEW), Situational Awareness (SA), SSL Certificate Manager (SCM), Security Expert Service (SES), and Cloud Bastion Host (CBH)
Enterprise Applications	Blockchain Service (BCS), ForeCloud Stack (FCS), VoiceCall, and PrivateNumber Message&SMS (MSG&SMS), ROMA Connect (ROMA), SD-WANService (SD-WAN), Cloud Managed Network (CMN), HUAWEI CLOUD Welink (Welink), Meeting, and Dedicated Computing Cluster (DCC)
Internet of Things	IoT Device Access (IoTDA), IoTDP (IoTDP), Global SIM Link (GSL), IoT Analytics (IoTA), IoT Edge (IoTEdge), IoV Platform (IoV), IoT Campus Service (IoTC), and OceanConnectV2X (RPS)
Enterprise Intelligence	Image Search (ImageSearch), ModelArts (ModelArts), HUAWEI HiLens (HiLens), Graph Engine Service (GES), Video Ingestion Service (VIS), Cloud Search Service (CSS), Natural Language Processing Fundamentals (NLPF), Language Understanding (Language Understanding), Language Generation (Language Generation), Natural Language Processing Customization (NLPC), Machine Translation (MT), Map Reduce Service (MRS), Cloud Stream Service (CS), Data Lake Insight (DLI), Data Warehouse Service (DWS), CloudTable Service (CloudTable), Data Ingestion Service (DIS), One-stop Data Governance Platform (DAYU), Data Lake Visualization (DLV), Recommender System (RES), Optical Character Recognition (OCR), Content Moderation (Moderation), Moderation (Text) (Moderation (Text)), Moderation (Image) (Moderation (Image)), Video Content Moderation (VCM), Face Recognition (FRS), Image Tagging (Image Tagging), Celebrity Recognition (ROC), Question Answering Bot (QABot), Task Bot (TaskBot), Speech Analytics (CBSSA), CBS Customization (CBSC), Real-time ASR (Real-time ASR), Audio Speech Recognition (ASR), Text to Speech (TTS), Audio Speech Recognition Customization (ASRC), Video Content Recognition (VCR), Video Content Processing (VCP), Video Content Tags (VCT), Video Fingerprinting (VEP), TrafficGo (TrafficGo), CampusGo (CampusGo), HeatingGo (HeatingGo), EIHealth (EIHealth), EI_Industrial (EI_Industrial), and Network AI Engine (NAIE)

3 HUAWEI CLOUD CSA CAIQ Consensus Assessment Initiative Questionnaire

3.1 AIS Application & Interface Security

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's response
		Yes	No	N/A	
AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/ Software Development Lifecycle (SDLC)?	X			HUAWEI CLOUD has pursued the new DevOps process, which features rapid and continuous iteration capabilities, and integrated the Huawei security development lifecycle (SDL). In addition, 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.

AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			HUAWEI CLOUD introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. For more details, please refer to the *HUAWEI CLOUD Security White Paper*.
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?		X		HUAWEI CLOUD does not use manual source-code analysis. Automatic code analysis tools run as part of the HUAWEI CLOUD software development life cycle.
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			HUAWEI CLOUD has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. For example, cybersecurity assessment requirements are added to open source software selection in the selection analysis phase to strictly control the selection. During the use of third-party software, carry out related activities by taking the third-party software as part of services or solutions, and focus on the assessment of the integration of open source, third-party, and Huawei-developed software, or whether new security issues are introduced when independent third-party software is used in solutions.
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Before HUAWEI CLOUD products or services are released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding.

AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			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.
AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	X			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.
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			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 control in the application interfaces and databases used in the HUAWEI CLOUD environment.

AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			According to integrity control as 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), such as verifying the consistency of data checked by hash algorithm before and after storage to ensure that the stored data is uploaded data, and regularly relies on internal and external audits to verify Its effectiveness. For the integrity verification of the content data, the customer is responsible for the implementation of input and output verification control in the application interfaces and databases used in the HUAWEI CLOUD environment.
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			HUAWEI CLOUD will continue to embrace industry leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. For further information, please refer to the *HUAWEI CLOUD Security White Paper*.

3.2 AAC Audit Assurance & Compliance

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's response
		Yes	No	N/A	
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources, etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			HUAWEI CLOUD has established a formal and regular audit plan, including continuous and independent internal and external evaluation. Internal evaluation continuously track the effectiveness of security control measures, and external evaluation is audited as an independent auditor for reviewing the efficiency and effectiveness of implemented security controls.
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	X			The effectiveness of implementation of security operations is included in HUAWEI CLOUD's formal and regular audit plan. Regularly reviewed standards such as ISO 27001, CSA STAR certification, PCI DSS certification, SOC report, etc. would also review the security implementation of HUAWEI CLOUD.
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Customers can apply to download the latest compliance certificates and reports including ISO27001 and SOC from the HUAWEI CLOUD Trust Center. Tenants who agree to HUAWEI CLOUD Confidentiality Commitment Letter can download such resources.
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			HUAWEI CLOUD organizes internally or external third parties with certain qualifications to conduct penetration tests on all HUAWEI CLOUD systems and applications every six months, and follow up and rectify the results of penetration tests.

AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			According to the best practice of PCI DSS, HUAWEI CLOUD organizes internally or external third parties with certain qualifications to conduct penetration tests on all HUAWEI CLOUD systems and applications every six months, and follow up and rectify the results of penetration tests.
AAC-02.4	Do you conduct internal audits at least annually?	X			HUAWEI CLOUD has established a formal and regular audit plan, including continuous and independent internal and external evaluation, internal evaluation continuously track the effectiveness of security control measures, and external evaluation is audited as an independent auditor for reviewing the efficiency and effectiveness of implemented security controls. At the same time, HUAWEI CLOUD has obtained ISO27001 certification, which meets the requirements of internal audit every year, and the compliance is confirmed by a third party every year.
AAC-02.5	Do you conduct independent audits at least annually?	X			HUAWEI CLOUD has established a formal and regular audit plan, including continuous and independent internal and external evaluation, internal evaluation continuously track the effectiveness of security control measures, and external evaluation is audited as an independent auditor for reviewing the efficiency and effectiveness of implemented security controls. HUAWEI CLOUD conducts audits based on the standards of AICPA every year and releases related SOC reports, as well as annual review of a number of standards.

AAC-02.6	Are the results of the penetration tests available to tenants at their request?		X		Although HUAWEI CLOUD conducts penetration tests on a regular basis, and has a dedicated team to follow up the test results. The penetration test report and follow-up would be verified by internal audits and external certification agencies, but the report is not provided to tenants.
AAC-02.7	Are the results of internal and external audits available to tenants at their request?	X			HUAWEI CLOUD provides tenants with SOC audit reports issued by third-party audit institutions in accordance with the relevant standards of the American Institute of Certified Public Accountants (AICPA). Tenants who agree to HUAWEI CLOUD Confidentiality Commitment Letter can download the SOC audit report from the HUAWEI CLOUD Trust Center.
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			HUAWEI CLOUD has set up professional positions to maintain contact with external parties to monitor relevant laws and regulations. When new laws and regulations related to HUAWEI CLOUD services are released, HUAWEI CLOUD would promptly adjust internal security requirements and security controls, and follow up the compliance of laws and regulations.

3.3 BCR Business Continuity Management & Operational Resilience

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Yes	No	N/A	

BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			At present, 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.
BCR-01.2	Do you have more than one provider for each service you depend on?	X			In the disaster recovery strategy of HUAWEI CLOUD, it is stipulated that multiple suppliers should be used for the same service to cope with emergencies, so as to retain certain redundancy to maintain service continuity.
BCR-01.3	Do you provide a disaster recovery capability?	X			HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS), which can help customers quickly restore business at the disaster recovery site and shorten the business interruption time. This service helps protect business applications, replicates data and configuration information of the Elastic Cloud Server to the disaster recovery site, and allows the servers where the business applications run onstarted from another location and operate normally during the downtime, thereby improving business continuity.
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	X			In the disaster recovery strategy of HUAWEI CLOUD, it is stipulated that multiple suppliers should be used for the same service. When a program failure is detected, the service continuity of the upstream provider would be estimated. If the upstream provider's service is interrupted, it would be switched to another service provider in time.

BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?		X		HUAWEI CLOUD would not provide tenants with operational redundancy reports. However, HUAWEI CLOUD regularly conducts external third-party audits such as ISO 22301 and ISO 27001 certification to check the controls of disaster redundancy, and periodically tests the effectiveness of the redundancy mechanism internally.
BCR-01.6	Do you provide a tenant-triggered failover option?	X			The Storage Disaster Recovery Service (SDRS) provided by HUAWEI CLOUD provides one-click disaster recovery switching. When an event occurs or is needed, the business will be switched to the disaster recovery site to avoid business interruption caused by the event.
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?		X		HUAWEI CLOUD would not provide tenants with business continuity reports. However, HUAWEI CLOUD regularly conducts external third-party audits such as ISO 27001 certification every year to evaluate the business continuity plan, and internally tests the business continuity to maintain its effectiveness.
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			The HUAWEI CLOUD security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan. When significant changes take place in the organization and environment of HUAWEI CLOUD, the effectiveness of business continuity level would also be tested.

BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			HUAWEI CLOUD strictly follows the requirements of clause A11.2 related to equipment of ISO 27001 information security management system, adopts control measures to prevent the loss, damage, theft or endangering of assets and the interruption of organizational activities, and conducts annual audit on the implementation of this requirement every year.
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			HUAWEI CLOUD has implemented a backup and redundancy strategy, including position mutual preparation of internal, internal & external, and external, multiple offices in the same city or other places, redundant equipment and spare parts, and the use of multiple manpower, equipment, service providers, and development and testing environments, code document version management, tool software, safety equipment, backup and redundancy of production systems.
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			HUAWEI CLOUD has established information system related documents in accordance with international standards such as ISO27001 Information Security Management System, ISO27017 Cloud Computing Information Security Management System, ISO27701 Privacy Information Management System, and authorized employees can access the corresponding documents.
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			In terms of physical protection, HUAWEI CLOUD has established zone protection. To reduce risks, a location selection strategy has been formulated for possible natural disasters. For risks such as intrusion and authorization a monitoring and response mechanism has been established as well.

BCR-06.1	Are any of your data centers located in places that have a high probability/ occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		HUAWEI CLOUD data center will consider selecting locations with stable politics, low crime rate and friendly environment, away from areas with hidden dangers of natural disasters such as floods, hurricanes, earthquakes, etc., avoiding strong electromagnetic field interference, and setting the minimum distance for the hidden dangers area around the technical requirements.
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			For the maintenance of the data center, HUAWEI CLOUD has established system and process documents related to data center operation and maintenance management, including specific equipment management and control measures, routine maintenance plans, etc.
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	X			For the maintenance of the data center, HUAWEI CLOUD has established system and process documents related to data center operation and maintenance management, including specific equipment management and control measures, routine maintenance plans, etc.
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			HUAWEI CLOUD complies with Appendix A.17.2 of ISO 27001, which indicates that the information processing equipment should meet the availability requirements, and to avoid service interruption through equipment, network, supplier redundancy, and audits the implementation of this requirement every year to maintain ISO 27001 certification.

BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			Referring to the requirements of ISO22301, HUAWEI CLOUD uses indicators such as RPO, RTO, success rate of disaster recovery, success rate of backup and success rate of recovery to measure the achievement of disaster recovery goals. Service recovery priority and disaster importance are rated in the process of assessing the impact of the business interruption.
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			HUAWEI CLOUD uses RPO, RTO, success rate of disaster recovery, success rate of backup and success rate of recovery to measure the achievement of disaster recovery goals. Service recovery priority and disaster importance are rated in the process of assessing the impact of the business interruption.
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			According to the requirements of ISO 27001, HUAWEI CLOUD has formulated business continuity management regulations, incident response strategy and process. All these documents are provided for all relevant employees to read, and key positions in the response process need to be trained and regular drills.
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	X			HUAWEI CLOUD *Customer Agreement and Privacy Statement* inform customers of their personal data retention policies. HUAWEI CLOUD has the technical capabilities to implement the retention policies in the above agreements. For customers' content data, they can configure their own content data retention policies, and HUAWEI CLOUD strictly follows customer instructions to process their content data.

BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			HUAWEI CLOUD has established management policies for the data retention mechanism, in which HUAWEI CLOUD needs to compliance with the minimum or maximum retention period required by law and applies different disposal methods for different types of personal data.
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Except for Identity and Access Management (IAM)/ Object Storage Service (OBS,) the management data (including operation logs, etc.) of all launched services and components on HUAWEI CLOUD would be backed up to OBS. At the same time, the management data of IAM/OBS needs to be backed up to non-OBS storage. Customers can use Cloud Backup and Recovery (CBR) service to backup servers, cloud hard drives, and virtualized environments in the cloud.
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Customers can use the Cloud Eye Service (CES) to monitor the running status of the server and the resources on the cloud in real time. When a hardware failure occurs, CES will notify the customer via email, SMS, and HTTP/S. At the same time, customers can use the snapshot function in the Elastic Volume Service (EVS) to fully restore the data to the snapshot time point in case of data losing.
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	X			HUAWEI CLOUD provides Image Management Service (IMS) which can be used to backup the instance of cloud server for customers. When the software environment of the instance fails, the backup image can be used to restore.

BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	X			HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS), which can help customers quickly restore business at the disaster recovery site and shorten the business interruption time.
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	X			HUAWEI CLOUD would regularly test the validity of the user's management data backup. For customers' content data, customers need to develop their own backup and redundancy mechanisms according to business needs, and test the effectiveness of the mechanism.

3.4 CCC Change Control & Configuration Management

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Yes	No	N/A	
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			HUAWEI CLOUD uses DevOps and DevSecOps models for development, and has formulated corresponding management systems and procedures to control development and change activities. For further information, please refer to the *HUAWEI CLOUD Security White Paper*.

CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			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.
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			HUAWEI CLOUD has established systematic change management and service launch process, communicating 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. In the external audits, such as ISO 27001, PCI DSS certification and SOC reports, the compliance of these controls has been reviewed.
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. HUAWEI CLOUD runs threat analysis based on the service scenarios, data flow diagrams, and networking models during the security requirement analysis and design phases, and specifies threat reduction plans. At the same time, all cloud services shall pass multiple rounds of security testing and code reviews before they are released. For the security of HUAWEI CLOUD development activities, please refer to the *HUAWEI CLOUD Security White Paper*.

CCC-03.2	Is documentation describing known issues with certain products/services available?	X			HUAWEI CLOUD announces the vulnerabilities of products or services that have been discovered on its official website and fore warns customers. Customers can check the **Security Notice** to be aware of the scope of the vulnerabilities, how to deal with them, and the threat level.
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			HUAWEI CLOUD has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures, and to disclose security vulnerabilities in the **Security Notice** on the official website of HUAWEI CLOUD.
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Before HUAWEI CLOUD service development and test personnel are on boarded, they are all required to learn corresponding specifications and prove they have learned these by passing examinations on them. HUAWEI CLOUD introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding, including but not limited to micro service-level functions and interface security tests such as authentication, authorization, and session security in the alpha phase; API and protocol fuzzing type of testing incorporated in the beta phase; and database security validation testing in the gamma phase.

CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?	X			HUAWEI CLOUD ensures the secure introduction and use of open source and third-party software based on the principle of strict entry and wide use. HUAWEI CLOUD has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. For example, cybersecurity assessment requirements are added to open source software selection in the selection analysis phase to strictly control the selection.
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			HUAWEI CLOUD clearly stipulates that all authentication, credential data and business data in the test process shall be deleted before data and code enter the production environment, and the test code shall be deleted.
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			All computers needs to install the safe-defense software designated by HUAWEI CLOUD to monitor, and only software in the security software list specified by the company can be installed.
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		HUAWEI CLOUD does not provide this type of document to customers. While providing services and products to customers, HUAWEI CLOUD would continually optimize products. Major product changes would be notified to customers in accordance with the methods specified in the HUAWEI CLOUD *Customer Agreement*.

CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			HUAWEI CLOUD has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of HUAWEI CLOUD Change Committee.
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			HUAWEI CLOUD has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of HUAWEI CLOUD Change Committee. The change strategy of the production environment complies with the existing cloud service level agreement.

3.5 DSI Data Security & Information Lifecycle Management

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Yes	No	N/A	

DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/ instantiating/ transporting data in the wrong country)?	X			The Elastic Cloud Server (ECS) products provided by HUAWEI CLOUD include the function of adding tags. Tags are used to mark cloud resources such as instances, images, and disks. If there are multiple cloud resources under the customer's account, and there are multiple associations between different cloud resources, they can add tags to the cloud resources to realize the classification and unified management of cloud resources.
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/ metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		X		HUAWEI CLOUD only provides customers with virtual machines instead of hardware for delivery as a service, and does not support marking functions for hardware and data flow.
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?			X	HUAWEI CLOUD provides operational documents required for services, and customers decide the processing and use of data based on their service functions, relevant networks, system components and their own business needs.
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			The customer decides the available zones geographically where the content data store. HUAWEI CLOUD would not migrate customer content from selected areas without notifying customers, unless it's necessary to meet legal compliance or government requirements.

DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			HUAWEI CLOUD supports data transmission in REST and Highway modes: ● In REST mode, a service is published to the public as a RESTful service and the initiating party directly uses an HTTP client to initiate the RESTful API for data transmission. ● In Highway mode, a communication channel is established using a high-performing Huawei-proprietary protocol, which is best suited for scenarios requiring especially high performance. Both REST and Highway modes support TLS 1.2 for data in transit encryption and X.509 certificate-based identity authentication of destination websites. The SSL Certificate Management Service is a one-stop-shop type of X.509 certificate full lifecycle management service provided to our tenants by HUAWEI CLOUD together with world-renowned public Certificate Authorities (CA). It ensures the identity authentication of destination websites and secure data transmission.
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			API needs to use TLS encryption to ensure the confidentiality of transmission. At present, all APIs of the API gateway to the external network use TLS1.2 version encryption protocol, and support PFS (Perfect Forward Secrecy) security feature.

DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	For content data, customers should establish corresponding management and control strategies for the labeling and processing of their content data to ensure data security. Customers can use the Tag Management Service (TMS) to manage tags that identify resources in services such as Elastic Cloud Server (ECS), Virtual Private Cloud (VPC), Elastic Volume Service (EVS), etc., so as to achieve unified management of resource tags on the cloud.
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	For content data, customers should establish and follow structured data-labeling standard based on business requirements. HUAWEI CLOUD only processes data in accordance with customer instructions.
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	For content data, customers should establish a label inheritance mechanism suitable for their data.

DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			In order to prevent the production data from being moved or replicated to the non-production environment, HUAWEI CLOUD controls as follows: • Physical and logical network boundaries and strictly enforced change control policies; • Separation of responsibilities of employees in production and non-production environments; • Highly restrict physical and logical access to the cloud environment; • Continuous security, privacy and security coding practice awareness and training; • Continuously record and audit system access; • Conduct regular compliance audits to ensure control effectiveness.
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			HUAWEI CLOUD has established system requirements for data security management, in which data management responsibilities are defined and assigned, and employees with corresponding permissions can access the specific content of the system. When employees enter the company, they would conduct training and communication on their data management responsibilities, and confirm their understanding before they are on boarded.
DSI-07.1	Do you support the secure deletion (e.g., degaussing/ cryptographic wiping) of archived and backed-up data?	X			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.

DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			After confirming data deletion by users, HUAWEI CLOUD deletes the user data permanently to prevent data leakage, including memory deletion, data leakage prevention through encryption, deletion of stored data, disk data deletion and physical disk destruction. For further information, please refer to the *HUAWEI CLOUD Security White Paper*.

3.6 DCS Datacenter Security

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Yes	No	N/A	
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			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.
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			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.

DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of GB 50174 Code for Design of Electronic Information System Room and T3+ standard of TIA - 942 Telecommunications Infrastructure Standard for Data Centers. HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. 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 online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	X			HUAWEI CLOUD supports IP address-based access control. Users can choose whether to use IP addresses as authentication conditions in the Identity and Access Management (IAM) configuration.

DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?				HUAWEI CLOUD conducts equipment identification and management in accordance with ISO27001 requirements. HUAWEI CLOUD has obtained ISO27001 certification, and the certification can be downloaded from the Trust Center. Customers can use multi-factor authentication through IAM, which support methods include mobile phones, mailboxes, and virtual MFA etc.
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			The infrastructure undertaking the service operation is managed by authorized personnel in HUAWEI CLOUD's data center. The infrastructure of the data center, including the access and processing of storage medium, is managed in accordance with relevant medium management requirements.
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	X			Confidential policies and procedures of HUAWEI CLOUD are not directly provided to customers. HUAWEI CLOUD works with external certification agencies and independent auditors to review and verify its compliance with the policies.
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			The ISO27001 standard requires organizations to establish standards and procedures to maintain a safe and secure working environment in offices, rooms, facilities, and secure areas. HUAWEI CLOUD has obtained ISO27001 certification, and the certification can be downloaded from the Trust Center.

DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			The ISO27001 standard requires employees and third-party personnel to complete information security training. HUAWEI CLOUD has obtained ISO27001 certification, and the certification can be downloaded from the Trust Center.
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. 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 online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.

DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. 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 online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.

DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			HUAWEI CLOUD through access control systems, strictly review and regularly audit user access privileges. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system (WMS). Designated personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis to ensure that unauthorized personnel have no access to data centers.

3.7 EKM Encryption & Key Management

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Yes	No	N/A	
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	X			According to HUAWEI CLOUD Key Management Policy, each user has a unique ID that identifies them. Customers can use Key Management Service (KMS) of IAM to bind keys to identifiable owners.

EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			Customers can use HUAWEI CLOUD Data Encryption Workshop (DEW) for exclusive encryption, key management, and key pair management, which supports key creation, authorization, automatic rotation, and key hardware protection. Customers can choose their own key management mechanism according to their needs.
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	X			Data Encryption Workshop (DEW) supports customers to authorize HUAWEI CLOUD to host private keys.
EKM-02.3	Do you maintain key management procedures?	X			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.
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Data Encryption Workshop (DEW) provided by HUAWEI CLOUD 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 and record the ownership of keys.
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			To protect tenants' crypto keys and mitigate the risks of crypto key leakage to the public, HUAWEI CLOUD provides cloud HSM service using different HSM vendors in different specifications (such as industry standard encryption algorithms, and country-specific encryption algorithms) and cipher suite strengths, which allows tenants to select the options suitable for their real-world requirements, for example, third-party HSM certified by FIPS140-2.

EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			The customer is responsible for the encrypted storage of its content data. HUAWEI CLOUD's Data Encryption Workshop (DEW) can provide customers with encrypted storage functions in Elastic Volume Service (EVS), Object Storage Service (OBS), Volume Backup Service (VBS) and other services.
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			In the scenario where data is transmitted between clients and servers and between servers of the HUAWEI CLOUD via common information channels, data in transit is protected as follows: 1. VPN: The Virtual Private Network (VPN) service is used to establish a secure encrypted communication channel that complies with industry standards between a remote network and a tenant VPC such that a tenant's existing traditional data center seamlessly extends to HUAWEI CLOUD. Currently, HUAWEI CLOUD uses IPSec VPN together with Internet Key Exchange (IKE) to encrypt the data transport channel and ensure transport security. 2. Application-layer security: TLS and certificate management: HUAWEI CLOUD supports data transmission in REST and Highway modes. Both REST and Highway modes support TLS 1.2 for data in transit encryption and X.509 certificate-based identity authentication of destination websites.
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			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.

EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			HUAWEI CLOUD itself uses the AES strong encryption method widely used in the industry to encrypt data in the platform, and uses a high-level TLS encryption protocol to ensure data security during transmission. Customers can use Data Encryption Services to encrypt data. HUAWEI CLOUD provides cloud HSMs of different vendors, specifications (standard encryption algorithms, national encryption algorithms, etc.), and different strengths for tenants to choose to meet the needs of different tenants.
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			HUAWEI CLOUD supports key management methods selected by customers. HUAWEI CLOUD provides HSMs of different vendors, specifications (standard encryption algorithms, national secret algorithms, etc.), and different strengths for tenants to choose to meet the needs of different tenants.
EKM-04.3	Do you store encryption keys in the cloud?	X			KMS enables users to manage their keys conveniently and ensures the security of critical business data by supporting data encryption using a data encryption key (DEK) at any time. The DEK is encrypted using the customer master key (CMK) that is stored in KMS. Key disclosure is prevented by storing the root key of the KMS in the HSM. The root key at no time appears outside the HSM. In addition, at least two HSM devices are deployed as a pair to ensure reliability and availability. The CMKs are encrypted using the root key and saved as ciphertext on the key storage nodes.
EKM-04.4	Do you have separate key management and key usage duties?			X	Customers are responsible for their key management responsibilities assignment, and records of the use permission and control rights of the keys.

3.8 GRM Governance and Risk Management

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			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 and hardware). HUAWEI CLOUD establishes an internal technical standard specification library, which contains the information security baselines for every component in the infrastructure.
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			HUAWEI CLOUD requires that all services must pass the basic security requirements verification ahead of the release to ensure compliance with the infrastructure.

GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			According to the ISO27001 standard, HUAWEI CLOUD conducts information security risk management, and regularly performs information security risk assessments. Risk assessments cover all aspects of information security, including data protection and classification, data retention and transmission locations, and data retention time in compliance with laws and regulations. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			According to the ISO27001 standard, HUAWEI CLOUD conducts information security risk management, and performs information security risk assessments at least once a year. Risk assessments cover all aspects of information security, including data protection and classification, data retention and transmission locations, and data retention time in compliance with laws and regulations. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.

GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			Huawei regards cyber security as one of the company's important strategies, which is achieved through a top-down governance structure. In terms of organization, HUAWEI CLOUD establishes a cybersecurity management organization to decide and approve the company's overall cybersecurity strategy. At the same time, cyber security is included in the employee's business code of conduct, and the company's requirements for all employees in the field of cybersecurity are conveyed through annual employee business code of conduct learning, examinations, and signing activities, so as to improve employee cyber security awareness and sign a cybersecurity commitment letter, and promise to abide by the company's various network security policies and system requirements.
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			HUAWEI CLOUD does not directly provide customers with confidential information security management procedures. HUAWEI CLOUD invites third-party organizations to evaluate the information security management procedures of HUAWEI CLOUD and confirm that its operation complies with ISO27001 standards. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			According to the requirements of the ISO27001 standard, HUAWEI CLOUD invites third-party organizations to review the information security management plan ISMP every year. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.

GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			According to the requirements of ISO27001, HUAWEI CLOUD has clarified its own information security goals, formulated corresponding information security plans, and allocated the resources required to perform information security activities. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/ function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			According to the requirements of ISO27001 and SOC2, HUAWEI CLOUD implements documented information security policies and procedures to provide guidance for HUAWEI CLOUD's operations and information security. Employees can view the published information security policies and procedures under authorization. ISO 27001 and SOC related certificates and reports can be obtained from the Trust Center.

GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			According to ISO27001 requirements, the leadership of HUAWEI CLOUD establishes information security goals, formulates corresponding information security plans, and allocates resources required to perform information security activities. The information security plan meets the requirements of customers and HUAWEI CLOUD itself. HUAWEI CLOUD has passed ISO27001 certification, and related certificates can be obtained from the Trust Center.
GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			When HUAWEI CLOUD introduces suppliers, all suppliers will sign confidentiality and service level agreements with HUAWEI CLOUD. The agreement contains requirements for the supplier's security and privacy data processing.
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			HUAWEI CLOUD displays the obtained certifications in the trust center, and published a number of white papers related to regulations and standards. The white paper introduced the mapping and compliance between HUAWEI CLOUD's control and regulatory requirements. For details, please refer to **the Trusted Resources** page on the official website of HUAWEI CLOUD.
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			The controls, standards, certifications, and regulations that HUAWEI CLOUD complies with have all been published in **theTrust Center** of HUAWEI CLOUD official website.

GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Huawei has established a strict security responsibility system and implemented an accountability mechanism for violations. HUAWEI CLOUD holds employees accountable on the basis of behavior and results. According to the nature of HUAWEI CLOUD employees' security violations and the consequences, the accountability handling levels are determined and handled in different ways. Those who violate laws and regulations shall be transferred to judicial organs for handling. Direct managers and indirect managers shall assume management responsibilities if they have poor management or knowingly inaction. The handling of violations will be aggravated or mitigated according to the attitude of the individual who violated the regulations and the cooperation in the investigation.
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			HUAWEI CLOUD's violation management policies are published internally for all employees to view and learn. And HUAWEI CLOUD regularly organizes training to improve employees' understanding of violations, consequences of violations, and punitive measures.
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			HUAWEI CLOUD will update security policies, procedures, standards, and controls every year based on risk assessments results to maintain their effectiveness and relevance.
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			When the security and privacy policies have significant changes, HUAWEI CLOUD will formally notify the designated contact customers through the reserved contact information.

GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			HUAWEI CLOUD will review its privacy and security policies every year to evaluate whether they meet compliance and effectiveness.
GRM-10.1	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			HUAWEI CLOUD has developed information security risk assessment methods, which determine the possibility and impact of all identified risks through qualitative and quantitative methods, and judges the severity of the risk based on the possibility and impact. The methods will be conducted annually in accordance with ISO27001 requirements.
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			According to the requirements of ISO27001, HUAWEI CLOUD formulates the information security risk assessment method to identify risks from multiple dimensions and judges the possibility of risks based on the completeness of security strategies, security technologies, and security audits.
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			According to ISO27001 requirements, HUAWEI CLOUD has established an information security risk management program that is applicable within HUAWEI CLOUD organization to reduce and manage risks. The information security risk management program is regularly reviewed and updated by the specified department.
GRM-11.2	Do you make available documentation of your organization-wide risk management program?	X			During auditing the compliance with standards such as PCI DSS and ISO27001, external certification institutions will review the risk management plans and implementations of HUAWEI CLOUD.

3.9 HRS Human Resource Security

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			HUAWEI CLOUD has issued personnel security relevant management regulations, requiring employees to transfer their HUAWEI CLOUD assets to the company when they resign or leave their posts. When the contract/business relationship with the partner is terminated, the information generated in the cooperation project in the self-contained device should be deleted according to the cooperation agreement, and the assets provided by HUAWEI CLOUD will be returned.
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	X			HUAWEI CLOUD has established an electronic flow of assets transfer when personnel resign/termination of cooperation, and implement assets transfer in accordance with the electronic process.
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Under the permission of applicable laws, HUAWEI CLOUD will conduct background checks on employees, contractors, or other third parties based on the confidentiality of accessible assets.

HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities.
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			Newly hired or employed 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.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			HUAWEI CLOUD internally released personnel security relevant management regulations, providing employees with security management policies and process support before, during, and at the end of the employment relationship.
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			It is an automatic electronic flow to revoke access rights when personnel resign or leave the posts. The human resources department and IT department follow up the return of organizational assets.

HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			HUAWEI CLOUD has formulated regulations for managing mobile devices, requiring that confidential positions are not allowed to equip laptops. When a laptop enters a controlled area, it needs to be approved, and the laptop needs to take measures to prevent data leakage in case of loss.
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			HUAWEI CLOUD's professional legal department manages and regularly reviews the details of the confidentiality agreement to maintain the confidentiality agreement to meet the needs of business operations.
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			HUAWEI CLOUD introduced the HUAWEI CLOUD shared responsibility model in the *HUAWEI CLOUD Security White Paper*. For HUAWEI CLOUD, as a cloud service provider, and its customers, the security management responsibility is assumed separately. This document can be obtained from the trusted resources in the Trust Center.

HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			HUAWEI CLOUD separately stipulated the usage quotas for terminal equipment, network and system components, and explained the monitoring strategy for quotas.
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			HUAWEI CLOUD only allows employees to install applications on their personal phones to access company mailboxes, forums and other functions, and controls the access scope of applications according to employee permissions.
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			HUAWEI CLOUD conducts security awareness trainings for all employees, implements corresponding cybersecurity fundamental trainings for different types of employees, conducts tailored training for typical security associate responsible persons, and empowers security training and enablement for key positions. For more detailed information, please refer to the *HUAWEI CLOUD Security White Paper*.

HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			HUAWEI CLOUD incorporates cybersecurity into code of business conduct for employees. Through annual employee business code of conduct learning, examinations, and signing activities, HUAWEI CLOUD conveys the company's requirements for all employees in the field of cybersecurity, improves employees' awareness of cybersecurity, and signs a letter of commitment to cybersecurity, promising to abide by the company's various network security policies and system requirements.
HRS-09.3	Do you document employee acknowledgment of training they have completed?	X			HUAWEI CLOUD keeps records of activities such as the study, examination and signing of employee business codes of conduct, and signing of cybersecurity commitments each year, which are reviewed by internal and external audits each year.
HRS-09.4	Is successful and timed completion of the training program (s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			For employees involved in sensitive data, systems, procedures and other key positions such as network security and privacy protection, they must undergo induction training and achieve corresponding certifications, and sign confidentiality commitment letters and confidentiality agreements.
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	X			HUAWEI CLOUD incorporates cybersecurity into code of business conduct for employees. Through annual employee business code of conduct learning, examinations, and signing activities, HUAWEI CLOUD conveys the company's requirements for all employees in the field of cybersecurity, improves employees' awareness of cybersecurity, and signs a letter of commitment to cybersecurity, promising to abide by the company's various network security policies and system requirements.

HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			HUAWEI CLOUD conducts security awareness trainings for all employees, implements corresponding cybersecurity fundamental trainings for different types of employees, conducts tailored training for typical security associate responsible persons, and empowers security training and enablement for key positions. For more detailed information, please refer to the *HUAWEI CLOUD Security White Paper*.
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			HUAWEI CLOUD incorporates cybersecurity into code of business conduct for employees. Through annual employee business code of conduct learning, examinations, and signing activities, HUAWEI CLOUD conveys the company's requirements for all employees in the field of cybersecurity, improves employees' awareness of cybersecurity, and signs a letter of commitment to cybersecurity, promising to abide by the company's various network security policies and system requirements.
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			According to the requirements of SOC, PCI DSS, ISO27001 and other standards, HUAWEI CLOUD has established regulations on the responsibilities and behaviors of employees, and third-party audit agencies will review whether employees are informed of their job responsibilities for maintaining information security.
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			According to the requirements of SOC, PCI DSS, ISO27001 and other standards, HUAWEI CLOUD has established regulations on the responsibilities and behaviors of employees, and third-party audit agencies will review whether employees are notified of their work responsibilities to ensure equipment safety.

HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			According to the requirements of SOC, PCI DSS, ISO27001 and other standards, HUAWEI CLOUD has established regulations on the responsibilities and behaviors of employees. Third-party audit agencies will review whether HUAWEI CLOUD will configure all computers and laptops to ensure to lock the screen after a predefined time.
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			According to the requirements of SOC, PCI DSS, ISO27001 and other standards, HUAWEI CLOUD has established regulations on the responsibilities and behaviors of employees. Third-party audit agencies will check whether HUAWEI CLOUD has policies and procedures to ensure that there are no publicly visible sensitive documents in the unattended work area (For example, on the desktop).

3.10 IAM Identity & Access Management

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. Customers can use IAM to restrict access permissions, and use the Cloud Log Service (CLS) to record access and modification records for sensitive information or security configurations.

IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			HUAWEI CLOUD uses the log system to monitor administrator-level access and control that non-administrator employees do not have more than their due permissions, such as privileged access.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			HUAWEI CLOUD has established access control management requirements in accordance with the requirements of ISO27001. It follows the principle of permissions minimization and the principle of permissions separation. The employees' permissions scope has been regularly reviewed to avoid permissions exceeding their work scope. When an employee's on-the-job status changes, the permissions shall be cleaned and modified in time. Logs of employees' logins and operations will be kept for the required time to respond to audit requirements.
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/ assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			HUAWEI CLOUD has established access control management requirements in accordance with the requirements of ISO27001. It follows the principle of permissions minimization and the principle of permissions separation. The employees' permissions scope has been regularly reviewed to avoid permissions exceeding their work scope. When an employee's on-the-job status changes, the permissions shall be cleaned and modified in time. Logs of employees' logins and operations will be kept for the required time to respond to audit requirements.

IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			HUAWEI CLOUD has established access control management requirements in accordance with the requirements of ISO27001. It follows the principle of permissions minimization and the principle of permissions separation. The employees' permissions scope has been regularly reviewed to avoid permissions exceeding their work scope. When an employee's on-the-job status changes, the permissions shall be cleaned and modified in time. Logs of employees' logins and operations will be kept for the required time to respond to audit requirements.
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			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. Take data storage as an example, HUAWEI CLOUD's block storage, object storage, file storage and other services all regard customer data isolation as an important feature. Take block storage as an example, data isolation is performed in units of volumes (cloud hard drives), and each volume is associated a customer ID. The virtual machine that mounts the volume must also have the same customer ID to complete the mounting of the volume to ensure customer data isolation.

IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			HUAWEI CLOUD provides each employee with a unique identity and setting permissions based on job responsibilities. Employees' identity will be verified every time they log in, so that HUAWEI CLOUD can trace the logs in time for accountability in an accident. HUAWEI CLOUD IAM can help customers implement AAA rules and support the cloud platform's identity verification, authorization, and accountability mechanisms.
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			HUAWEI CLOUD emphasizes that the security risks of employee cloud service accounts are controllable, strong security passwords are strictly required, account permissions are regularly reviewed, and privileged accounts are strictly managed and recycled. Employees must use multi-factor authentication to confirm their identity every time they log in.
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			HUAWEI CLOUD's Cloud Monitoring Service monitors the operation of the system that the customer is using, regardless of the status of the system. After the system is deleted, the access to the system will no longer be monitored.
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. All access to ports, applications, system components, etc. are only open to authorized individuals and applications.

IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			HUAWEI CLOUD's internal IAM system is responsible for the management of the entire life cycle of employees, storing and managing their identity information, positions, access rights, and account types.
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			HUAWEI CLOUD's internal IAM system is responsible for the management of the entire life cycle of employees, storing and managing their identity information, positions, access rights, and account types.
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Customers can refer to the best practices in the HUAWEI CLOUD IAM product documentation to formulate their own duties separation strategy and safe usage of IAM. The document provides resource authorization management and permission setting cases for customers' reference.
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. All access to ports, applications, system components, etc. are only open to authorized individuals and applications.

IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			HUAWEI CLOUD has established access control management requirements in accordance with the requirements of ISO27001. It follows the principle of permissions minimization and the principle of permissions separation. The employees' permissions scope has been regularly reviewed to avoid permissions exceeding their work scope. When an employee's on-the-job status changes, the permissions shall be cleaned and modified in time. Logs of employees' logins and operations will be kept for the required time to respond to audit requirements.
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	X			HUAWEI CLOUD manages third-party suppliers in accordance with ISO27001 requirements, and signs confidentiality and service level agreements with third-party suppliers. The agreement contains requirements for security and privacy data processing, and management of their access permissions should not exceed those necessary for their services.
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			HUAWEI CLOUD assigns permissions to employees based on the principle of least permission. Unless necessary, employees will not be given the permission to access customer content data and their all access operations will be logged.
IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. All access to ports, applications, system components, etc. are only open to authorized individuals and applications.

IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. All access to ports, applications, system components, etc. are only open to authorized individuals and applications.
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	X			HUAWEI CLOUD assigns permissions to employees according to the minimum scope of working needs. The access and modification of the information security management system and sensitive information are under monitored and recorded. All access to ports, applications, system components, etc. are only open to authorized individuals and applications.
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			HUAWEI CLOUD provides each user with a separate account, evaluates employees' job responsibilities and work content before they are on board, and provides, manages, and reviews employees' permissions based on the principle of minimizing permissions.

IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			HUAWEI CLOUD provides each user with a separate account, evaluates employees' job responsibilities and work content before they are on board, and provides permissions for employees based on the principle of minimizing permissions, including access to data, applications, fundamental architecture and network components within the scope of permissions.
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			Consistent with the relevant requirements of the ISO27001 standard, HUAWEI CLOUD provides employees with the minimum permissions based on their work needs, and reviews the permissions every year, so that system users and administrators always follow the principle of minimum permissions. HUAWEI CLOUD will maintain the ISO27001 certificate every year and continue to comply with the requirements of the standard.
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			Consistent with the relevant requirements of the ISO27001 standard, HUAWEI CLOUD provides employees with the minimum permissions based on their work needs, and reviews the permissions every year, so that system users and administrators always follow the principle of minimum permissions. HUAWEI CLOUD will maintain the ISO27001 certification every year and the compliance with requirements of the standard.

IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	X			Consistent with the relevant requirements of the ISO27001 standard, HUAWEI CLOUD provides employees with the minimum permissions based on their work needs, and reviews the permissions every year, so that system users and administrators always follow the principle of minimum permissions. HUAWEI CLOUD will maintain the ISO27001 certification every year and the compliance with requirements of the standard.
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?		X		Customers are responsible for the access control of their own data and ensure that their access permissions are set effectively to avoid improper access. HUAWEI CLOUD strictly abides by the principle of tenant isolation, and data between different tenants is logically isolated from each other. HUAWEI CLOUD's privileged user access control has passed SOC, ISO27001 and PCI DSS certification audits every year.
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			After the status changes, such as resignation or position change, employees and other third parties shall conduct a security according to the transfer and resignation safety review checklist, which includes the clearance or modification of the resignation account permissions.

IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			After the status changes, such as resignation or position change, employees and other third parties shall conduct a security review according to the transfer and resignation safety review checklist, which includes the clearance or modification of the resignation account permissions.
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Currently, Huawei Cloud supports two forms of federal identity authentication: ● Webpage single sign-on (WebSSO): The browser is used as a communication medium and is suitable for ordinary users to access HUAWEI CLOUD through the browser. ● Calling API interface: Development tools/applications are used as communication media, such as OpenStackClient and Shibboleth ECPClient, suitable for enterprises or users to access HUAWEI CLOUD through API calls.

IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			HUAWEI CLOUD supports single sign-on based on the SAML2.0 protocol. Customers can use the identity provider function to enable users to log in to HUAWEI CLOUD using an enterprise identity provider account. Currently, Huawei Cloud supports two forms of federal identity authentication: ● Webpage single sign-on (WebSSO): The browser is used as a communication medium and is suitable for ordinary users to access HUAWEI CLOUD through the browser. ● Calling API interface: Development tools/applications are used as communication media, such as OpenStackClient and Shibboleth ECPClient, suitable for enterprises or users to access HUAWEI CLOUD through API calls.
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/ authorizing users?	X			HUAWEI CLOUD supports single sign-on based on the SAML2.0 protocol. Customers can use the identity provider function to enable users to log in to HUAWEI CLOUD using an enterprise identity provider account. Currently, Huawei Cloud supports two forms of federal identity authentication: ● Webpage single sign-on (WebSSO): The browser is used as a communication medium and is suitable for ordinary users to access HUAWEI CLOUD through the browser. ● Calling API interface: Development tools/applications are used as communication media, such as OpenStackClient and Shibboleth ECPClient, suitable for enterprises or users to access HUAWEI CLOUD through API calls.

IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			X	Customers should set constraints and control rules for their access permissions in accordance with their applicable laws and regulations, and manage account permissions through IAM.
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			Customers can manage account permissions through IAM, set roles and groups according to specific business needs, and configure account locking strategies, password complexity strategies, multi-factor authentication and other functions according to security requirements.
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			HUAWEI CLOUD's IAM Service supports the use of multi-factor authentication for login verification and operation protection. After the login verification function is enabled, when the user logs in to the console, in addition to the user name and password, the verification code must be entered on the login verification page; after the operation protection is enabled, the user needs to enter the verification code to confirm the operation when performing sensitive operations. Multi-factor authentication devices support mobile phones, mailboxes and virtual MFA devices.

IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			HUAWEI CLOUD supports single sign-on based on the SAML2.0 protocol. Customers can use the identity provider function of HUAWEI CLOUD to enable users to log in to HUAWEI CLOUD using an enterprise identity provider account. Currently, HUAWEI CLOUD supports two forms of federal identity authentication: ● Webpage single sign-on (WebSSO): The browser is used as a communication medium and is suitable for ordinary users to access HUAWEI CLOUD through the browser. ● Calling API interface: Development tools/applications are used as communication media, such as OpenStackClient and Shibboleth ECPClient, suitable for enterprises or users to access HUAWEI CLOUD through API calls.
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			HUAWEI CLOUD's IAM Service supports policies of setting password complexity and modification period and etc. The customer's IAM administrator can set password policies as needed, such as the minimum password length, the maximum number of consecutive occurrences of the same character in the password, and the password cannot be the same as the historical password.

IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			HUAWEI CLOUD's IAM Service supports setting account lock, deactivation and other policies. If the number of failed logins is reached within a limited time, the account will be locked for a period. After the lockout period expires, the account can be logged in again. The tenant administrator can set the account lockout policy, which is effective for the account and the IAM users under the account. If the IAM account does not access HUAWEI CLOUD through the UI console or API within the set validity period, it will be disabled. The account can be re-enabled by contacting the administrator.
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			When a customer administrator uses the HUAWEI CLOUD unified identity authentication service IAM to create a new user, he can send a one-time login link to the new user by email. The new user needs to set a password when logging in using the link. In addition, the customer administrator customizes the new user's password can choose to force the user to modify the default password after activation. Both methods can prevent IAM users from using the default password.
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			HUAWEI CLOUD's IAM Service supports setting account lock, deactivation and other policies. If the number of failed logins is reached within a limited time, the account will be locked for a period. After the lockout period expires, the account can be logged in again. The tenant administrator can set the account lockout policy, which is effective for the account and the IAM users under the account. If the IAM account does not access HUAWEI CLOUD through the UI console or API within the set validity period, it will be disabled. The account can be re-enabled by contacting the administrator.

IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc.) appropriately restricted and monitored?	X			Only limited standard software can be installed on HUAWEI CLOUD office computers. Programs that exceed system, object, network, virtual machine, and application control measures are not allowed to be installed, and software installation is monitored.

3.11 IVS Infrastructure & Virtualization Security

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			HUAWEI CLOUD uses IPS intrusion prevention system, web application firewall, anti-virus software, and HIDS host-based intrusion detection system for vulnerability management of system components and networks. The IPS intrusion prevention system can detect and prevent potential network intrusion activities; Web application firewalls are deployed at the network boundary to protect the security of application software and protect it from external SQL injection, CSS, CSRF and other application-oriented attacks; Anti-virus software provides virus protection and firewall in Windows system; HIDS host-based intrusion detection system protects the security of cloud servers, reduces the risk of account theft, provides weak password detection, malicious program detection, two-factor authentication, vulnerability management, and webpage prevention Functions such as tampering.

IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			HUAWEI CLOUD assigns employees' access permissions in accordance with the principle of minimizing permissions, and employees can only access authorized content. Access and review permissions for logs are limited to specific employees, and the approval of their permissions needs to receive the approval of the superior management, and review them regularly.
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/ processes has been performed?	X			HUAWEI CLOUD displayed the obtained certifications in the Trust Center, and published a number of white papers related to regulations and standards. The white paper introduced the mapping and compliance between HUAWEI CLOUD's control and regulatory requirements. For details, please refer to **the Trusted Resources** page on the official website of HUAWEI CLOUD.
IVS-01.4	Are audit logs centrally stored and retained?	X			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.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			HUAWEI CLOUD has a dedicated internal audit department that regularly audits various activity logs of the operation and maintenance process.
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			HUAWEI CLOUD enables security logs for network devices and application systems that provide services. The logs will record all changes to devices and systems.

IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/ configuration of the virtual machine?	X			HUAWEI CLOUD provides customers with Cloud Audit Services. Customers can use cloud log services to record virtual machine configuration and logs changes, and use cloud audit services to monitor the integrity of configured logs.
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			Customers can use the Host Security Service (HSS) to check the integrity of the mirrored file, and use the comparison method to in HSS determine whether the current file status is different from the state when the file was scanned last time. Use this comparison to determine whether the file has valid or suspicious modifications. When potential risks are discovered, HUAWEI CLOUD will reminded customers in time.
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			HUAWEI CLOUD uses the NTP4.2.8 protocol to synchronize the time in the system.
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/ scenarios?	X			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.
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			HUAWEI CLOUD has established a complete resource management mechanism to plan the capacity of the resources in HUAWEI's unified virtualization platform to avoid excessive use of resources and meet customer capacity requirements.

IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			HUAWEI CLOUD has established a complete resource management mechanism to plan the capacity of the resources in HUAWEI's unified virtualization platform to avoid excessive use of resources and meet customer capacity requirements.
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			HUAWEI CLOUD collects component capacity information and system performance of cloud services to monitor the stable operation of the platform, and continues to meet the regulations, contracts, and business requirements of all systems used to provide services to tenants.
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			In view of the diversified means and huge traffic of public cloud attacks, HUAWEI CLOUD uses a situational awareness analysis system to correlate the alarm logs of various security devices and perform unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred.
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			HUAWEI CLOUD has released the *HUAWEI CLOUD Security White Paper* and *HUAWEI CLOUD Data Security White Paper* on the official website, provides solution consulting services covering a variety of industries and scenarios, and provide customers with multiple security architecture guidance.

IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/ zones?	X			HUAWEI CLOUD has a professional network security team who are responsible for updating the network architecture diagram and checking firewall rules between regions. In the annual review of HUAWEI CLOUD PCI DSS certification, this content will also be audited by a third-party organization.
IVS-06.3	Do you regularly review for appropriateness the allowed access/ connectivity (e.g., firewall rules) between security domains/zones within the network?	X			HUAWEI CLOUD has a professional network security team who are responsible for updating the network architecture diagram and checking firewall rules between regions. In the annual review of HUAWEI CLOUD PCI DSS certification, this content will also be audited by a third-party organization.
IVS-06.4	Are all firewall access control lists documented with business justification?	X			All firewall controls and change records are recorded in the security log, and the firewall configuration can only be changed after approval by a specific administrator.

IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			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: Huawei's professional Anti-DDoS equipment is deployed at the boundary of each cloud data center to complete the detection and cleaning of abnormal and large traffic attacks. ● Network intrusion detection and interception: IPS has real-time network traffic analysis and blocking capabilities, and can prevent various intrusions such as abnormal protocol attacks, brute force attacks, port/vulnerability scanning, viruses/trojans, and attacks against vulnerabilities. Based on network traffic, IPS can provide information to help locate and investigate network anomalies, allocate directional traffic restriction strategies, and adopt corresponding custom detection rules to ensure the security of applications and network infrastructure in the production environment. ● Web security protection: HUAWEI CLOUD deployed a web application firewall to respond to web attacks, such as DDoS attacks at the web application layer, SQL injection, cross-site scripting attacks, cross-site request forgery, component vulnerability attacks, and identity forgery.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			For customers of SaaS and PaaS products, HUAWEI CLOUD supports them to use virtual private cloud VPC services to establish an isolated production and test environment process on the cloud.

IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			HUAWEI CLOUD has released the *HUAWEI CLOUD Security White Paper* and *HUAWEI CLOUD Data Security White Paper* on the official website, provides solution consulting services covering a variety of industries and scenarios, and provide customers with multiple security architecture guidance.
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			HUAWEI CLOUD uses a combination of physical and logical control isolation methods for production and non-production environments, and controls the combined isolation methods to improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal ghosts.
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			HUAWEI CLOUD deploys the DoS/DDoS prevention cleaning layer, next-generation firewall, intrusion prevention system layer, and website application firewall layer at the network boundary. Internally, the data center is divided into multiple security areas based on business functions and network security risks, realizing physical and logical Control and use isolation methods to improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal ghosts.

IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			HUAWEI CLOUD deploys the DoS/DDoS prevention cleaning layer, next-generation firewall, intrusion prevention system layer, and website application firewall layer at the network boundary. Internally, the data center is divided into multiple security areas based on business functions and network security risks, realizing physical and logical Control and use isolation methods to improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal ghosts.
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			In order to ensure that tenant business does not affect management operations and ensure that equipment, resources and traffic will not deviate from effective supervision, HUAWEI CLOUD divides the communication plane of its network into tenant data plane and business control based on different business functions, different security risk levels, and different permissions. Plane, platform operation and maintenance plane, BMC management plane, data storage plane, etc., to ensure that network communication traffic related to different services is reasonably and securely shunted, which facilitates separation of duties.

IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			When customers use cloud hard drives, object storage, cloud databases, container engines and other services, HUAWEI CLOUD uses different granular access control mechanisms such as volumes, storage buckets, database instances, and containers to ensure that customers can only access their own data. In scenarios where customers build their own storage, such as installing database software on virtual machine instances, it is recommended that customers use HUAWEI CLOUD's virtual private cloud (VPC) services to build a private network environment, and use subnet planning, routing policy configuration, etc. to implement network areas Divide, place the storage in the internal subnet, and strictly control the network traffic in and out of the subnet and virtual machines by configuring network ACLs and security group rules.
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			HUAWEI CLOUD's isolation of cloud data is implemented through a virtual private cloud VPC, which uses network isolation technology to achieve complete isolation between different tenants on the three-layer network. Tenants can fully control the construction and configuration of their own virtual network: On the one hand, combined with VPN or cloud dedicated lines, connect the VPC and the traditional data center of the tenant's intranet to realize the smooth migration of tenant applications and data from the tenant's intranet to the cloud; On the one hand, by using the ACL and security group functions of the VPC, security and access rules can be configured on demand to meet the tenants' fine-grained network isolation needs.

IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			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 encrypted with AES-256.
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			In the process of migration of application or data, customers should consider using a network isolated from the production environment.
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			HUAWEI CLOUD enforces strict access control on HUAWEI CLOUD administrators who access the host operating system, and implements comprehensive log audits of all operations and maintenance operations performed by them. HUAWEI CLOUD administrators must pass two-factor authentication before they can access the management plane through the bastion machine. All operations will be logged and sent to the centralized log audit system in time.

IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	The infrastructure of the cloud platform does not involve the wireless network environment.
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	The infrastructure of the cloud platform does not involve the wireless network environment.
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	The infrastructure of the cloud platform does not involve the wireless network environment.
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			HUAWEI CLOUD maintains and updates its own network architecture diagram, and the team responsible for network security tracks and confirms the compliance of the network architecture.

IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			HUAWEI CLOUD deploys the DoS/DDoS prevention cleaning layer, next-generation firewall, intrusion prevention system layer, and website application firewall layer at the network boundary. Internally, the data center is divided into multiple security areas based on business functions and network security risks, realizing physical and logical Control and use isolation methods to improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal ghosts.

3.12 IPY Interoperability & Portability

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Tenants can obtain a list of all APIs provided in the publishing service through the **HUAWEI CLOUD API** list on the official website.
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			When customers' personal data collected by HUAWEI CLOUD is requested to export by customers themselves, HUAWEI CLOUD can provide data in standard formats commonly used in the industry according to customer needs.

IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			X	Customers are responsible for interoperability with third-party applications by themselves.
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			HUAWEI CLOUD Data Migration Service provides an industry-wide virtual machine image format, which supports saving to the customer's local data center. Customers need to complete the image migration work by themselves.
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		X		HUAWEI CLOUD has not provided such a service level agreement yet.
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			HUAWEI CLOUD uses TLS1.2 to encrypt the access and the data transmission process of management services, and the data will be encrypted using AES-256 when importing and exporting.
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			HUAWEI CLOUD provides customers with product documents and API interface documents for Cloud Data Migration Services. Customers can refer to the documents for portability related information in the service.

IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			HUAWEI CLOUD uses virtualization platforms widely used in the industry, such as KVM, Xen, Docker, etc., to reduce customers' learning costs.
IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			HUAWEI CLOUD provides customers with migration service of databases, file storage, and object storage, and migration from different regions and clouds to customer data centers.
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		X		HUAWEI CLOUD manages and tracks the modifications on existing virtual machines and provides these records to third-party organizations for auditing regularly, but this part of the content is not provided to customers for review.

3.13 MOS Mobile Security

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	

MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	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 responsive 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.
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	Same as MOS-02.1 question reply
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	Same as MOS-02.1 question reply
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	Same as MOS-02.1 question reply
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X	Same as MOS-02.1 question reply

MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	Same as MOS-02.1 question reply
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	Same as MOS-02.1 question reply
MOS-08.1	Do you have a BYOD policy that defines the device (s) and eligibility requirements allowed for BYOD usage?			X	Same as MOS-02.1 question reply
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X	Same as MOS-02.1 question reply
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	Same as MOS-02.1 question reply

MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	Same as MOS-02.1 question reply
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X	Same as MOS-02.1 question reply
MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	Same as MOS-02.1 question reply
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	Same as MOS-02.1 question reply
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	Same as MOS-02.1 question reply
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	Same as MOS-02.1 question reply

MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	Same as MOS-02.1 question reply
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	Same as MOS-02.1 question reply
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			X	Same as MOS-02.1 question reply
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	Same as MOS-02.1 question reply
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	Same as MOS-02.1 question reply
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	Same as MOS-02.1 question reply
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	Same as MOS-02.1 question reply
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	Same as MOS-02.1 question reply

MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	Same as MOS-02.1 question reply
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	Same as MOS-02.1 question reply
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	Same as MOS-02.1 question reply
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	Same as MOS-02.1 question reply
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	Same as MOS-02.1 question reply

3.14 SEF Security Incident Management, E-Discovery, & Cloud Forensics 82

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	

SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			According to the requirements of the ISO27001 standard, HUAWEI CLOUD is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies. HUAWEI CLOUD has been verified and certified by an independent audit institution to confirm compliance with the ISO27001 certification standard.
SEF-02.1	Do you have a documented security incident response plan?	X			HUAWEI CLOUD's incident response procedures, plans, and procedures are formulated in accordance with the ISO27001 standard. HUAWEI CLOUD has been verified and certified by an independent audit institution to confirm compliance with the ISO27001 certification standard.
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	X			HUAWEI CLOUD has formulated a general security incident response plan and process, including the responsibilities division, response speed, and public announcement mechanism of relevant personnel. Customers should develop an applicable incident response plan based on their needs.

SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			HUAWEI CLOUD released *the HUAWEI CLOUD Security White Paper*, which introduced that HUAWEI CLOUD is mainly responsible for the response to security incidents. To ensure the professionalism, urgency, and traceability of security event handling, HUAWEI CLOUD has comprehensive security log management requirements, security event rating and handling processes, a 24/7 professional security event response team, and a corresponding security expert resource pool. HUAWEI CLOUD strives to achieve rapid security incident response in terms of incident detection, impact scoping, damage isolation, and service recovery. In addition, HUAWEI CLOUD keeps security event rating criteria, time to response, and time to resolution up to date by taking into account the impact of a security event or incident on our entire network and customers.
SEF-02.4	Have you tested your security incident response plans in the last year?	X			In the past year, HUAWEI CLOUD conducted simulation exercises on security incidents in different fields to test the effectiveness of the plan.

SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			The management process of information security incidents established by HUAWEI CLOUD defines the responsibilities of each role. HUAWEI CLOUD conveys the company's requirements for all employees in the field of cybersecurity through the company's unified annual routine learning, examination and signing activities, and improves employee cybersecurity awareness. Employees are required to sign a cybersecurity commitment letter and promise to comply with the company's various cybersecurity policies and regulations. For other external related personnel, HUAWEI CLOUD signed confidentiality agreements with them and conducted information security training, which included information security incident reporting responsibilities.
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			HUAWEI CLOUD provides security announcements and vulnerability feedback pages on the official website to notify customers of the latest security vulnerability alerts and provide channels for customers to report security vulnerabilities.
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			HUAWEI CLOUD has established a security incident response plan and process in accordance with the requirements of ISO27001, ISO27017 and other standards, and regularly analyzes and checks the compliance of the security incident response plan in the countries and regions that have been served.

SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			HUAWEI CLOUD has established a security incident response plan and process in accordance with the requirements of ISO27001, ISO27017 and other standards, and regularly analyzes and checks the compliance of the security incident response plan in the countries and regions that have been served.
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			HUAWEI CLOUD has established a security incident response plan and process in accordance with the requirements of ISO27001, ISO27017 and other standards, and regularly analyzes and checks the compliance of the security incident response plan in the countries and regions that have been served.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			HUAWEI CLOUD has established a security incident response plan and process in accordance with the requirements of ISO27001, ISO27017 and other standards, and regularly analyzes and checks the compliance of the security incident response plan in the countries and regions that have been served.
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			HUAWEI CLOUD has established an incident management platform to record and track the progress, handling measures and implementation of all information security incidents, and analyzed the impacts after the incidents handling.
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		X		HUAWEI CLOUD's cloud services have clear responsibilities boundaries, and usually the security incident data is not shared with tenants. HUAWEI CLOUD provides complete security service products. After tenants configure according to their own business conditions, they can conduct related security events monitoring and data collection through security service products.

3.15 STA Supply Chain Management, Transparency, and Accountability

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			HUAWEI CLOUD collaborates with multiple departments and related suppliers to jointly maintain the quality management control and risk control measures of customer personal data in the life cycle of the supply chain, such as transactions, delivery, and service level monitoring. For details, please refer to the *HUAWEI CLOUD Data Security White Paper*. HUAWEI CLOUD will not check the quality of the content data of customers. 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.
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			HUAWEI CLOUD has formulated supplier security management requirements, and regularly reviews suppliers to verify whether theymeet HUAWEI CLOUD security and privacy standards.

STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			HUAWEI CLOUD has formulated a complete security incident response plan and process. When a security incident is triggered, HUAWEI CLOUD will carry out incident disposal in a timely manner, and HUAWEI CLOUD will provide all affected customers with security incident information through on-site notifications and emails.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			HUAWEI CLOUD collects component capacity information of cloud services to monitor the stable operation of the platform, and uses this information to optimize and upgrade cloud services.
STA-03.2	Do you provide tenants with capacity planning and use reports?	X			Customers can purchase the HUAWEI CLOUD enterprise service monthly report and check monthly summary reports that include cloud resource operation status and service support, as well as optimization suggestions based on HUAWEI CLOUD best practices. Customers can also monitor cloud services, capacity, and network usage by themselves through the Cloud Monitoring Service. The cloud monitoring service supports the reporting of custom indicators through OpenAPI, SDK, and Agent, and customers will be notified in time when a warning is triggered.
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			HUAWEI CLOUD has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators. In addition, independent third-party assessment agencies also provide independent assurance. These auditors assess the security, integrity, and confidentiality of information and resources by performing regular security assessments and compliance audits or inspections (such as SOC, ISO standards, PCIDSS audits), so as to conduct independent assessment of risk management content/process.

STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			HUAWEI CLOUD has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation to manage the supplier's compliance with the specific requirements and contract obligations of HUAWEI CLOUD.
STA-05.2	"Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			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.
STA-05.3	Does legal counsel review all third-party agreements?	X			The contract signed between HUAWEI CLOUD and the supplier needed to go through multiple rounds of contract review processes, and the content of it is reviewed by the HUAWEI CLOUD legal team.
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			Supplier security and privacy requirements are included in the signed contract agreement. Business personnel docking with third parties are responsible for managing their third-party relationships, including asset protection requirements and supplier access to related applications.
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			HUAWEI CLOUD provides tenants with a Cloud Server Backup Service. Through this service, tenants can create consistent online backups of all cloud hard drives under the cloud server. In response to scenarios such as virus intrusion, human deletion, software and hardware failures, etc., data can be restored to any backup point.

STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			The customer is responsible to select the availability zone of the specific geographic location where the content data is stored. HUAWEI CLOUD will not move customer content from selected regions without notifying the customer, unless required to comply with laws or government entity requirements.
STA-05.7	Can you provide the physical location/ geography of storage of a tenant's data upon request?	X			The customer is responsible to select the availability zone of the specific geographic location where the content data is stored. The name of the availability zone will identify the country and city where it is located.
STA-05.8	Can you provide the physical location/ geography of storage of a tenant's data in advance?	X			The customer is responsible to select the availability zone of the specific geographic location where the content data is stored. The name of the availability zone will identify the country and city where it is located.
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			The customer is responsible to select the availability zone of the specific geographic location where the content data is stored.
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			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.
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		HUAWEI CLOUD needs to detect customer access to metadata to calculate bills based on usage.

STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		HUAWEI CLOUD temporarily does not provide customers with sub-processors and copies of their agreements.
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			HUAWEI CLOUD has formulated supplier security management requirements, and regularly reviews suppliers to verify whether they meet HUAWEI CLOUD security and privacy standards. The review includes risk management and governance processes.
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			HUAWEI CLOUD has established a supplier selection and supervision system to manage suppliers' compliance with HUAWEI CLOUD's specific requirements and contract obligations through due diligence before contract signing and regular evaluation after contract signing.
STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/ downstream)?	X			HUAWEI CLOUD has established a supplier selection and supervision system to manage suppliers' compliance with HUAWEI CLOUD's specific requirements and contract obligations through due diligence before contract signing and regular evaluation after contract signing. HUAWEI CLOUD legal team will also review the terms of the contract regularly.
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			HUAWEI CLOUD follows the supplier selection and supervision system, requiring suppliers to provide uniform service level requirements and supervising their compliance.

STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			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.
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			HUAWEI CLOUD provides customers with Cloud Monitoring Services to help customers continuously monitor cloud services, capacity, and network usage. It supports the reporting of custom indicators through OpenAPI, SDK, and Agent, and customers will be notified in time when warnings are triggered.
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			HUAWEI CLOUD provides customers with Application Performance Management (APM) and Application Operation and Maintenance Management (AOM) services. APM is a cloud service that can real-time monitor and manage enterprise application performance and faults. AOM is a cloud operation and maintenance platform for operation and maintenance, development, operation personnel and IT managers. It real-time monitors operation and operation data in the form of logs, indicators, and events. Hundreds of operation and maintenance indicators for the entire link of cloud resources, networks, middleware, and cloud services are provided to customers.
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?			X	This question is not related to HUAWEI CLOUD service.
STA-07.8	Do you review all service level agreements at least annually?	X			HUAWEI CLOUD legal team regularly reviews SLAS. For the currently available SLA, please refer to: **Service Level Agreement** page.

STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			HUAWEI CLOUD has formulated supplier security management requirements and reviewed the supplier management status during the annual ISO 27001 audit conducted by a third-party organization. HUAWEI CLOUD collects supplier audit reports to verify whether they meet HUAWEI CLOUD security and privacy standards.
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			HUAWEI CLOUD has formulated supplier security management requirements and reviewed the supplier management status during the annual ISO 27001 audit conducted by a third-party organization. HUAWEI CLOUD collects supplier audit reports to verify whether they meet HUAWEI CLOUD security and privacy standards.
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			HUAWEI CLOUD has formulated supplier security management requirements and reviewed the supplier management status during the annual ISO 27001 audit conducted by a third-party organization. HUAWEI CLOUD collects supplier audit reports to verify whether they meet HUAWEI CLOUD security and privacy standards.
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. And hired an external third party to conduct penetration test of HUAWEI CLOUD application and network every six months.

3.16 TVM Threat and Vulnerability Management 92

No.	Consensus Assessment Questions	Consensus Assessment Answers			HUAWEI CLOUD's Response
		Y	N	N/A	
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			All office computers of HUAWEI CLOUD need to install the safe-defense software specified by the company, and only software from the specified software list can be installed. For IT basic systems and components, they are protected by IDS/IPS.
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			All office computers of HUAWEI CLOUD need to install company-designated safe-defense software, Anti-virus software and other security software need to be installed on infrastructure components. And the configuration modification rights of security software and require mandatory updates are restricted.
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Consistent with the relevant requirements of the PCI DSS standard, HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. And hired an external third party to conduct penetration test of HUAWEI CLOUD application and network every six months.

TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			Consistent with the relevant requirements of the PCI DSS standard, HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. And hired an external third party to conduct penetration test of HUAWEI CLOUD application and network every six months.
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			Consistent with the relevant requirements of the PCI DSS standard, HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. And hired an external third party to conduct penetration test of HUAWEI CLOUD application and network every six months.
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?		X		HUAWEI CLOUD will be responsible for the disposal of follow up the results of the vulnerability scan, and the results will not be provided to tenants.
TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			For all security vulnerability information known, HUAWEI CLOUD will evaluate and analyze each vulnerability, formulate and implement vulnerability fix plans or circumvention measures, and verify the fix situation after fixed, and continue tracking to confirm that the risk is eliminated or mitigated.

TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			X	HUAWEI CLOUD does not use tenant content data as part of the service. When HUAWEI CLOUD discovers vulnerabilities or other security incidents that may affect the security of tenant content data, it will notify the customer of the corresponding matters based on the provisions in the contract signed with the customer.
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	All office computers of HUAWEI CLOUD need to install the safe-defense software specified by the company. Only software from the specified software list can be installed, and Mobile code is not supported.
TVM-03.2	Is all unauthorized mobile code prevented from executing?	X			All office computers of HUAWEI CLOUD need to install the safe-defense software specified by the company. Only software from the specified software list can be installed, and Mobile code is not supported.

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
2020-09-30	1.0	First Publication