HUAWEI CLOUD Compliance with ISO 27001

Issue **2.2**

Date **2024-08-02**

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and its products and services available in HUAWEI CLOUD International website and the data center nodes that carry these products and services.

1.2 Purpose of Publication and Target Audience

ISO/IEC 27001 issued by the International Organization for Standardization (ISO), is an internationally accepted and widely used standard for information security management system (ISMS). The standard could be used to help organizations design and build information security management system. ISO 27001 focuses on risk management and regularly evaluates risks and controls to ensure the continuous operation of the organization's ISMS.

HUAWEI CLOUD has built a comprehensive information security managements system based on ISO/IEC 27001, developed the overall information security policy of HUAWEI CLOUD, and obtained the ISO/IEC 27001 certification.

This document describes HUAWEI CLOUD's overall information security policies and specific control measures by responding to the requirements of ISO/IEC 27001:2022 and the 4 themes and 93 control domains in Appendix A, helping customers understand：

- Main control requirements of ISO/IEC 27001:2022 in various control domains and HUAWEI CLOUD's responses to the control requirements;
- HUAWEI CLOUD offers multiple products and services to customers to help them to comply with ISO/IEC 27001:2022.

1.3 Basic Definitions

- **HUAWEI CLOUD**

  HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.
- **Customer (Tenant)**

Refers to the registered users who build business relationships with HUAWEI CLOUD. In this whitepaper, customers have the same meaning of tenant which indicates the user organization that use the services provided by HUAWEI CLOUD. The term “tenant” is used in some scenarios in this document.

- **International Organization for Standardization**

  ISO is an independent, non-governmental international organization with a membership of more than 160 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

- **SOD**

  "SOD" is often used as an abbreviation for "Separation of Duties". SOD refers to the separation of responsibilities and rights between business departments and business operators of an enterprise.

2 ISO 27001 Introduction

2.1 Framework and Main Contents of ISO 27001

ISO/IEC 27001 is the most widely used international information security management system guidance standard and best practice. It set out requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system within the organization and for the assessment and management of information security risks in accordance with the needs of the organization.

The new version of ISO/IEC 27001:2022 was officially released on October 25, 2022. ISO/IEC 27001:2022 Information Security, cybersecurity and privacy protection - Information security management systems - Requirements consists of two main parts: the requirements and Appendix A. The requirements part provides recommendations for information security management for initiating, implementing and maintaining security in the organization. Appendix A describes the requirements for establishing, implementing, and documenting an Information Security Management System (ISMS) and specifies the requirements for implementing security controls based on the needs of independent organizations. The major changes between this version and the 2013 version are as follows:

- The title is changed from ISO/IEC 27001:2013 Information Technology-Security Technology-Information Security Management System-Requirements to ISO/IEC 27001:2022 Information Security, Cyber Security, and Privacy Protection-Information Security Management System-Requirements.
- The text structure of the standard is slightly adjusted (level-2 and level-3 catalogs), including addition, expansion, and sequence adjustment. The text description of the standard is partially modified, but only clarified and properly expanded, and there is no requirement for addition or deletion.
- The title of Appendix A is changed to "Information Security Control Measures Reference", which refers to the information security control described in ISO/IEC 27002:2022. The 14 key domains of the previous version are combined into 4 security themes, namely, organization, personnel, physics, and technology.
- In Appendix A, 11 items are added, 58 items are updated, and 24 items are combined. A total of 93 items.

The control requirements in Appendix A are summarized into four themes that, when properly implemented, can help organizations achieve and maintain information security compliance by addressing specific issues identified in formal, periodic risk assessments.

The classification of the four themes in ISO/IEC 27001:2022 is based on the following:

- A 5 Organizational controls: Otherwise they are categorized as organizational.
- A6 People controls: if they concern individual people.
- A7 Physical controls: if they concern physical objects.
- A8 Technological controls: if they concern technology.

2.2 Applicable Organization of Standard

The requirements set out in ISO/IEC 27001:2022 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

3 The Certification Status of HUAWEI CLOUD

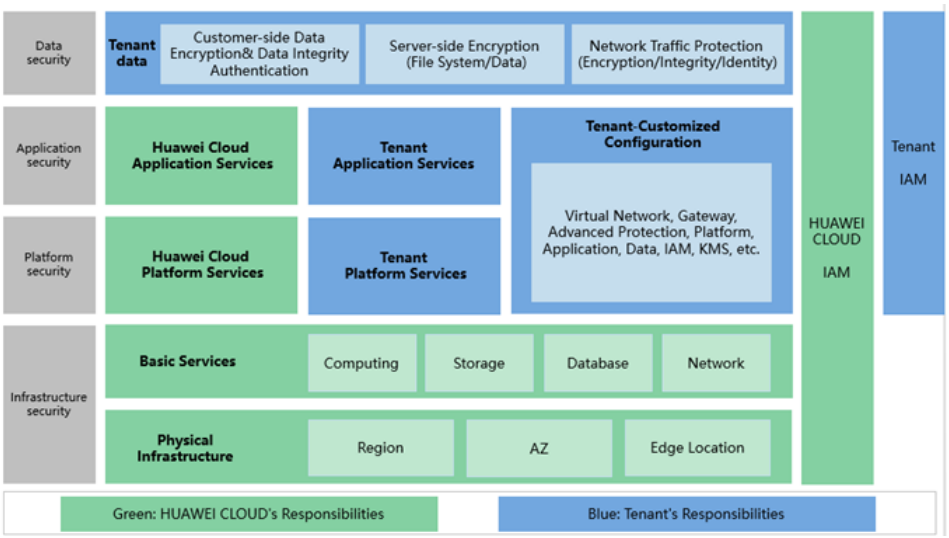
With its own information security system and security control management, HUAWEI CLOUD has obtained the ISO/IEC 27001:2022 certification. The certification covers products and services released by HUAWEI CLOUD on its official website, as well as data centers around the world.

For details about the certification scope and activity of ISO/IEC 27001:2022, see the certificate of registration available on HUAWEI CLOUD **Trust Center- Compliance**.

4 HUAWEI CLOUD Security Responsibility Sharing Model

Due to the complex cloud service business model, cloud security is not the sole responsibility of one single party, but requires the joint efforts of both the tenant and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenants to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the tenant and HUAWEI CLOUD:

图4-1 **Responsibility Sharing Model**



As shown in the above model, the privacy protection responsibilities are distributed between HUAWEI CLOUD and tenants as below:

HUAWEI CLOUD: The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical,

infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross-layer function.

Tenant: The primary responsibilities of the tenants are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant subscribes on HUAWEI CLOUD, including its customization of HUAWEI CLOUD service according to its needs as well as the O&M of any platform, application, and IAM services that the tenant deploys on HUAWEI CLOUD. At the same time, the tenant is also responsible for the customization of the security settings at the virtual network layer, the platform layer, the application layer, the data layer, and the cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the effective management of its users and identities.

For details on the security responsibilities of both FIs and HUAWEI CLOUD, please refer to the **HUAWEI CLOUD Security White Paper** released by HUAWEI CLOUD.

5 How HUAWEI CLOUD Meets ISO 27001 Requirements

5.1 ISO 27001 Requirement

HUAWEI CLOUD establishes and implements the information security management system (ISMS) according to ISO 27001, and maintains and continuously improves the system according to the PDCA cycle model in daily operations. In the initial phase of system establishment, the internal and external environment is determined, and the requirements of related parties are identified to determine the scope of the information security through a top-down governance structure. The leadership decides and approves information security policies and objectives, information security-related roles and responsibilities, formulates corresponding information security plans, allocates resources required for information security activities, and provides support for other roles in the system. Promote continuous improvement of the system. To facilitate smooth communication with external parties, HUAWEI CLOUD has dedicated personnel to keep in touch with administrative agencies, risk and compliance organizations, local authorities and regulatory agencies and establish contact points.

According to the ISO 27001 information security management system requirements, HUAWEI CLOUD has established information system documents, including documented information security policies and procedures, to guide HUAWEI CLOUD operations and information security management. Employees can access published information security policies and procedures as authorized. The information security management system documents are reviewed at least once a year and updated as needed to reflect changes in business objectives or risk environments. Changes to information security policies and procedures require management approval.

HUAWEI CLOUD has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security, including data protection and classification, data retention and transmission locations, and compliance with laws and regulations for the duration of data retention. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan. The risk assessment report is approved by management upon completion.

HUAWEI CLOUD has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. New employees must pass information security and privacy protection training and exams before passing the probation.

On-duty employees need to select courses to study and take exams based on their business roles. The training frequency for general employees is at least once a year, and the training frequency for core employees is higher. Managements must attend information security training and workshops. To address security awareness, HUAWEI CLOUD provides training for all employees to help them understand the organization's information security policies and regulations. In addition, employees must promise to comply with the company's security policies and regulations.

HUAWEI CLOUD has established a formal and regular audit plan, including continuous and independent internal and external assessments. Internal evaluation continuously tracks the effectiveness of security control measures, and the external evaluation is audited as independent auditors for reviewing efficiency and effectiveness of implemented security controls. In addition, HUWEI CLOUD regularly conducts management reviews every year, identifies problems in the system operation, and implements rectifications to promote continuous improvement of the management system.

5.2 ISO 27001 Annex A (normative) Reference controls

5.2.1 A.5 Organizational controls

No.	Control Domain	Control	HUAWEI CLOUD's response
A.5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at intervals and if significant changes occur.	Huawei Cloud has established and implemented documented cybersecurity policies and procedures to provide guidance for operational cybersecurity management. Cybersecurity policies and procedures must be approved by managers before they are released, and employees can view the policies and procedures based on their authorization. Additionally, Huawei Cloud regularly conducts employee training every year in terms of company policies and culture. The cybersecurity management policies and procedures are reviewed at least once a year and updated as needed to reflect changes in business objectives or risk environments by Huawei Cloud. Changes to information security policies and procedures require management approval. At the same time, Huawei Cloud has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators, and report the results and recommendations of the investigation to the top management.
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated	From an organizational structure perspective, the top management of HUAWEI CLOUD is responsible for making decisions on and approving the overall security strategy of the company wide. HUAWEI CLOUD Security

		according to the organization needs.	Management Department is responsible for enact and implement HUAWEI CLOUD end-to-end cybersecurity protection system. HUAWEI CLOUD Security Management Department is responsible for the implementation of major event backtracking for regular review to ensure that the policies, specifications, and specific measures of security governance are implemented in the process of various business fields, and realize end-to-end security governance. Additionally, HUAWEI CLOUD has clearly stipulated the cybersecurity responsibilities of all employees in the business team of each product and service. HUAWEI CLOUD has set up roles specifically responsible for security and privacy protection to assume certain security management responsibilities. Cybersecurity-related roles and responsibilities are identified in writing and approved by the top management.
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Huawei Cloud specifies the cybersecurity responsibilities of all employees in the business teams of products and services. Huawei Cloud assigns security and privacy protection roles to assume security management responsibilities. Cybersecurity-related roles and responsibilities are identified in writing and approved by the top management. Huawei Cloud complies with the separation of duties (SOD) and rights checks and balances principles to separate incompatible responsibilities to achieve proper rights division. In addition, the SOD management matrix is developed to help implement the SOD management principles.
A.5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	HUAWEI CLOUD has formulated information security management requirements for general employees, employees in confidential positions, and external personnel. For employees, the employment agreement signed with HUAWEI shall include confidentiality clauses and specify employees' information security responsibilities. For external personnel, the contact department of HUAWEI CLOUD shall specify information security management requirements for external personnel and the company to which they belong, as well as

			punishment measures for information security violations in the contract or agreement signed with them.
A.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	HUAWEI CLOUD has dedicated personnel to maintain contact with industry organizations, risk and compliance organizations, local authorities, and regulators. In regions within our cloud service coverage, Huawei Cloud actively facilitates dialogue with local regulators to better understand their concerns and requirements, share Huawei Cloud's knowledge and experience, and continue to bolster the legal and regulatory compliance posture of Huawei Cloud's technologies, services, and security
A.5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	HUAWEI CLOUD has dedicated personnel to maintain contact with industry organizations, risk and compliance organizations, local authorities, and regulators. In regions within our cloud service coverage, Huawei Cloud actively facilitates dialogue with local regulators to better understand their concerns and requirements, share Huawei Cloud's knowledge and experience, and continue to bolster the legal and regulatory compliance posture of Huawei Cloud's technologies, services, and security
A.5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Huawei CLOUD closely monitors industry-reputable vulnerability databases, security forums, email distribution lists, industry security conferences and other channels to identify Huawei Cloud-related vulnerabilities close to real time. Huawei Cloud employs its situation awareness (SA) analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. SA incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks. In addition, the system performs real-time evaluation of the security posture of Huawei Cloud, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping Huawei Cloud take necessary security precautions.
A.5.8	Information security in	Information security shall be integrated into	HUAWEI CLOUD has developed a complete project management approach and is CCM5/ CMMI, ISO 9001:2000 and PMI

	project management	project management.	framework-based practices which have enabled successful project implementations over the world by qualified project and project management professionals. Huawei Cloud incorporates security objectives into project objectives in project management, assesses information security risks at the early stage of the project, and periodically reviews information security impacts throughout the project delivery process to ensure there is no negative impact on the organization's operations and security. Huawei Cloud implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, and etc. Huawei Cloud and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, Huawei Cloud runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Huawei Cloud regularly identifies hardware, software, data, personnel, and services. Huawei Cloud uses the Cloud Asset Management system to monitor the inventory and maintenance status of Huawei Cloud information assets recorded on the asset management platform in real time, classify, monitor, and manage information assets, and generate an asset list for each asset. In addition, In Huawei Cloud, configuration managers are assigned to manage the configuration of all services, the resource

			configuration model consists of hosts, service trees, cloud infrastructures, and network devices. Configuration item mapping and resource lifecycle management are constructed to ensure stable and secure O&M in production environment. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes. Huawei Cloud uses IPAM to centrally manage IP resources. In addition, the HSP host security platform suite is deployed on the Huawei Cloud platform to provide network security protection for platform assets.
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Huawei Cloud has developed and implemented asset usage regulations, including management principles, responsibilities of related personnel, office computer security requirements, office network security requirements, office application system security requirements, storage media and port security requirements, office peripheral security requirements, non-HUAWEI computer security requirements, and related penalties. Huawei Cloud has implemented hierarchical data management and graded data based on confidentiality integrity, availability, and compliance. Data is classified into multiple security levels and defined separately. It also specified security implementation requirements, audit requirements, emergency response, and drill requirements for different levels of data. Each business domain marks the security level of the data in its domain according to the data grading standards.
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	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 security review checklist, which includes the clearance or modification of the resignation account permissions. In addition, Huawei Cloud require employees to transfer their Huawei Cloud assets to the company when they transfer and resign. 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. 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. Huawei Cloud employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities.
A.5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Huawei Cloud uses the Cloud Asset Management (CAM) system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and create an asset list for each asset. In addition, In Huawei Cloud, configuration managers are assigned to manage the configuration of all services, the resource configuration model consists of hosts, service trees, cloud infrastructures, and network devices. Configuration item mapping and resource lifecycle management are constructed to ensure stable and secure O&M in production environment. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes. Huawei Cloud has implemented hierarchical data management and graded data based on confidentiality integrity, availability, and compliance. Data is classified into multiple security levels and defined separately. It also specified security implementation requirements, audit requirements, emergency response, and drill requirements for different levels of data. Each business domain marks the security level of the data in its domain according to the data grading standards.
A.5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification	Huawei Cloud has formulated asset management procedures, which specify the classification and grading methods of information assets and the authorization rules that should be followed for various types of assets. In addition, Huawei Cloud has established information asset confidentiality management requirements, which specify the confidentiality measures that Huawei Cloud should take for

		scheme adopted by the organization.	information assets at different levels, and standardize the use of assets to ensure that the company's assets are properly protected and shared and ensure assets are protected at the appropriate level according to their importance to the organization. Huawei Cloud uses the Cloud Asset Management (CAM) system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets. Huawei Cloud requires that storage media containing Huawei confidential information must be marked. Confidential data shall be marked or labeled according to the data security level, and the security level shall be stated.
A.5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	HUAWEI CLOUD has formulated security management regulations, defined information transmission policies and processes, and detailed control requirements. 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: -**Virtual Private Network (VPN)**: VPN 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 local data center seamlessly extends to HUAWEI CLOUD while ensuring end-to-end data confidentiality. With a VPN-based communication channel established between the traditional data center and the VPC, a tenant can utilize HUAWEI CLOUD resources such as cloud servers and block storage at one's convenience. Applications can be migrated to the cloud, additional web servers can be launched, and the compute capacity within a tenant space can be expanded so as to establish enterprise hybrid cloud architecture and also lower risks of unauthorized dissemination of a tenant's core business data. Currently, HUAWEI CLOUD uses IPsec VPN together with Internet Key Exchange (IKE) to encrypt the data transport channel and ensure transport security. -Application Layer TLS and Certificate

			Management: 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. **SSL Certificate Manager (SCM)** 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. HUAWEI CLOUD protects information sent in electronic messages by using office
A.5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	HUAWEI CLOUD employee account management complies with HUAWEI user account permission management regulations. For HUAWEI CLOUD cloud platform accounts, HUAWEI CLOUD has formulated public cloud account permission management requirements and processes. Manage accounts by category and establish access control policies. Related documents have passed the review process and been released. Based on different business roles and responsibilities, access permissions management applies RBAC and includes the following basic roles: core network, access network, security devices, service systems, database systems, hardware maintenance, and monitoring maintenance. Any O&M personnel is restricted to access only devices within the administrative scope of his/her role and is not granted permissions to access other devices.
A.5.16	Identity management	The full life cycle of identities shall be managed.	HUAWEI CLOUD employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. **Identity and Access Management (IAM)** is used to control and manage user access to

			cloud services. All O&M accounts, device accounts, and applications are managed in a unified manner to ensure the end-to-end management, including user creation, authorization, authentication, and permission reclaiming. If the account user wants to use the account, the account administrator can initiate the authorization process and authorize the account by using a password or increasing the account's permissions. The applicant and approver of the account cannot be the same person.
A.5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Huawei Cloud has formulated password policies and account security management regulations, including specifying the password length, complexity, and change period. Passwords cannot contain user IDs. Common passwords that are easily cracked and the latest five passwords cannot be used. These regulations manage the allocation of secret authentication information. The default password of an account in the new system is changed by the user before the first use. When the user needs to reset the password, the user identity is authenticated.
A.5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.	Huawei Cloud employees use a unique identity in the internal office network, and have established comprehensive account lifecycle management regulations and processes. A new employee must be approved and authorized by the president of the employing department and the department's HR. The management platform will create an account for the employee after approval, and the account is used for the employee to log in to various systems or platforms within Huawei Cloud. All Huawei Cloud O&M accounts are managed in a unified manner, monitored by the unified audit platform, and automatically audited. Huawei employee accounts and two-factor authentication are required for O&M personnel to access the Huawei Cloud management network from which systems are centrally managed. When a Huawei Cloud employee is transferred to another position, the transfer personnel must apply for the transfer and the e-flow will be automatically transferred to the department director where the employee belongs. The department director confirms with the system administrator and HR that the employee's current permissions

			have been canceled and confirms the employee's transfer in the e-flow. Before the employee's resignation e-flow completes, the e-flow must be reviewed by the department director and HR to ensure that the employee's permissions have been canceled and the employee's account will be automatically deregistered after the employee resigns. Huawei Cloud has specified the maximum review period for accounts/ rights at different levels. The account/right owner periodically reviews the accounts/rights held by the account/right owner and submits a deregistration application when the user is transferred or the role changed. The management owner submits a deregistration application when the outsourced personnel leaves the site or no longer needs the account or permission. The supervisor will review whether the subordinate's account/right is proper. If the subordinate's position/ role changes, the supervisor will review whether the subordinate's account/right of the original position has been cancelled.
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.	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.
A.5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Huawei Cloud has established a formal procurement audit process. Huawei Cloud requires sign contracts, service agreements, and non-disclosure agreements with suppliers before conducting on-site work. The contract and service agreement specify the responsibilities and obligations of both parties, and clarify the cyber security requirements, service content, and service level that the supplier should meet. In addition, the non-disclosure agreements restrict clauses that violate confidentiality. Supplier security and privacy requirements are included in the signed contract agreement. Third-party business contacts manage their third-party relationships, including asset protection requirements and vendor access to related applications.

			The Legal Department of Huawei Cloud reviews and updates the NDA every year to ensure that the NDA can continuously meet business requirements on supplier management.
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	When introducing suppliers, Huawei Cloud signs confidentiality and service level agreements with them. The agreements contain requirements for security and privacy data processing of suppliers. Furthermore, Huawei Cloud has formulated a supplier personal information protection policy, which clearly defines the privacy and data protection management requirements that suppliers should be followed.
A.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	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. 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. HUAWEI CLOUD has formulated general procurement change management regulations and processes to strictly manage supplier service changes according to the management regulations. HUAWEI CLOUD will notify customers in a timely manner when important suppliers change based on customer requirements.
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization’s information security requirements.	As a cloud service provider, Huawei Cloud ensures secure development, configuration, and deployment of cloud technologies and the security of the operation and management of cloud services. According to ISO 27001, ISO27017, ISO27018, SOC, and CSA STAR, Huawei Cloud has built a comprehensive information security management system and formulated the overall information security strategy of Huawei Cloud. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system documents and the key focus areas and objectives of information security. Huawei Cloud follows the established information security management system,

			including asset security, access control, cryptography, physical security, operational security, communication security, system secure development, supplier management, information security incident management, and business continuity. Huawei Cloud protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. Furthermore, Huawei Cloud Security Management Department periodically reviews the implementation of the policy to ensure that the cybersecurity governance policies, standards, specifications, and specific measures are implemented in the processes of each business area. Huawei Cloud Security Management Department regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.
A.5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Huawei Cloud has developed a mechanism for internal security incident management, standardized security incidents response operations, and clarified classification and escalation principle of security incidents mechanisms. The roles and responsibilities are clearly defined for each activity during the incident response process. Employees can view the policies and procedures based on their authorization. Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The system continuously and analyzes security events in time to detect events. To support the customer's requirement to share threat intelligence with stakeholders, Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services.

			Based on internal management requirements, HUAWEI CLOUD annually drills information security incident management procedures and processes through internal red-blue confrontation. All of information security incident response personnel, including reserve personnel, need to participate.
A.5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Huawei Cloud log analysis platform collects security logs of operation systems, servers, and network devices. In addition, the platform presets abnormal operation rules to identify abnormal operations, automatically generates alarms, and pushes the alarms to generate and analyzed by emergency response personnel. Abnormal alarms are handled in a timely manner according to service level agreements, and screen monitoring and recording through the incidents analysis and processing platform in real-time. Huawei Cloud security incident response team is responsible for incident monitor and record, and assess whether a security incident is, also they track and manage the collected security incident by unified management to ensure security incident can be fixed in time.
A.5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	HUAWEI CLOUD has developed a security event management mechanism to standardize HUAWEI CLOUD security event response operations. When a security event occurs, follow the HUAWEI CLOUD incident response process. (Identify, evaluate, make decisions, and execute emergency response) In, the emergency handling process of HUAWEI CLOUD cyber security incidents is specified. The detected security incidents can be handled, escalated, reported, and managed in a closed-loop manner in a timely manner, ensuring the availability, integrity, and confidentiality of HUAWEI CLOUD services. Response mechanisms are implemented based on security incidents of different types and levels. After an incident occurs, HUAWEI CLOUD responds to and resolves the incident within a specified time limit based on the incident priority, minimizing the impact of the incident on customers. HUAWEI CLOUD provides training and drills on information security incident management procedures and processes every year. All security incident response

			personnel, including backup personnel, must participate in the training. In addition, to ensure that the security incident response process is effectively executed, HUAWEI CLOUD formulates emergency plans (such as anti-tampering on official websites) for typical security scenarios and conducts drills every year. The emergency drill process and results will be recorded in an emergency drill report for business and security departments to analyze and optimize the security incident response process. HUAWEI CLOUD evaluates whether to update the emergency plan based on security scenario changes every year. Security experts review the emergency plan updates.
A.5.27	Information security incidents shall be responded to in accordance with the documented procedures.	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls	HUAWEI CLOUD has a professional security event management system to record and track the progress, handling measures, and implementation of all information security incidents, analyze the impact of incident handling, track and close security incidents in an end-to-end manner, ensure that the entire handling process is traceable, and generate incident reports to summarize lessons learned. Inform the incident description, cause, impact, and measures taken by HUAWEI CLOUD in the report, and periodically conduct event backtracking and root cause analysis with the owner of the intruded service or system to ensure that experience is learned to prevent similar security incidents from happening again. In addition, HUAWEI CLOUD reviews the handling of high-risk events every year to ensure that the handling of high-risk events meets the actual business requirements of Huawei.
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	HUAWEI CLOUD provides training and drills on information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training to ensure that major incidents can be handled in a timely manner. In addition, when a server or application is suspected to be intruded, security response personnel perform evidence collection analysis, and use the security event management system to record and archive security event evidence collection data, emergency response records, and investigation and analysis processes. HUAWEI CLOUD periodically

			collects statistics and analyzes the trend of events. For similar events, the problem handling team analyzes the root causes and formulates solutions to prevent such events from occurring.
A.5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Huawei Cloud established a business continuity management system, to standard business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. Huawei Cloud has obtained the certification of the ISO22301 business continuity management system standard, formulated a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP. Additionally, the Huawei Cloud security drill team regularly develops exercises for different product types (including basic services, operation centers, data centers, and organization, etc.) and drills in different scenarios to maintain the effectiveness of the continuity plan.
A.5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Huawei Cloud performs business impact analysis and risk assessment annually to identify critical activities and dependencies, assess risk levels, and develop response strategies for identified threats that may cause cloud service resource disruption and establish a business continuity plan. At the same time, Huawei Cloud adopts the redundancy mechanism of single-region multiple data centers for all cloud services within the scope of the business continuity management system to ensure the business continuity of cloud services. Huawei Cloud security drill team regularly develops exercises for different product types (including basic services, operation centers, data centers, and organization, etc.)

			and drills in different scenarios to maintain the effectiveness of the continuity plan. The emergency response plan is developed based on different emergency scenarios and emergency response processes that may be involved in each product. The business continuity team will perform a business continuity drill for each product within the audit scope according to the business continuity drill plan every year and issue a business continuity drill report accordingly. Huawei Cloud conducts business continuity publicity and training within the organization annually, periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP.
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Huawei Cloud specifies the compliance process in its cybersecurity policies and regularly identifies and records compliance requirements. In addition, Huawei Cloud has set up dedicated posts to maintain active contact with external parties to track changes in laws and regulations. When identifying laws and regulations related to Huawei Cloud services, Huawei Cloud will adjust internal security requirements and security control levels in a timely manner to track compliance with laws and regulations.
A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Huawei has formulated IPR management regulations, which specify that employees shall comply with Huawei's IPR and information security policies to protect and legally use Huawei's IPR. Huawei Cloud formulates and implements desktop terminal service software standards and open-source software lists, and only standard operating systems and software applications defined in the list can be used. The iDesk program on the terminal device has an approved applications whitelist, and Huawei Cloud internal office software can

			only be downloaded from this platform. The Huawei Cloud security team periodically reviews and updates the software whitelist to ensure the continuous validity of the whitelist to prevent information assets from being invaded by malware. In addition, HUAWEI CLOUD formulates trusted third-party software management mechanisms and evaluation standards to reduce security risks caused by third-party software and ensure the security of products and solutions.
A.5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	HUAWEI CLOUD has specified data classification standards, protection measures for data at all levels, and information asset confidentiality management requirements. HUAWEI CLOUD manages operation data assets by category and level, strengthens data security control, and avoids risks or losses caused by improper behavior. Defines data classification and different levels of sensitivity/openness, specifies data anonymization and labeling standards, and regulates security measures that must be followed during the data lifecycle. HUAWEI CLOUD takes proper protection measures and strictly implements them to ensure the security of audit records. HUAWEI CLOUD prevents unauthorized access, modification, and deletion of audit records by restricting access permissions. HUAWEI CLOUD regularly reviews and updates the established asset management process every year. In addition, HUAWEI CLOUD Security Management Department regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in processes of each business domain.
A.5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	HUAWEI CLOUD, as a cloud service provider, defines data security responsibility sharing model. The user agreement signed with the customer clearly defines the ownership, security responsibilities, and obligations of the customer and HUAWEI CLOUD data. HUAWEI CLOUD will protect customer procurement information in accordance with data retention clauses and privacy statements. During processing, HUAWEI CLOUD will collect, store, and use customer information in compliance with the data minimization principle, and take

			comprehensive data protection measures to ensure customer account information security. HUAWEI CLOUD has specified data classification standards, protection measures for data at all levels, and information asset confidentiality management requirements. HUAWEI CLOUD manages operation data assets by category and level, strengthens data security control, and avoids risks or losses caused by improper behavior. Defines data classification and different levels of sensitivity/openness, specifies data anonymization and labeling standards, and regulates security measures that must be followed during the data lifecycle. In addition, HUAWEI CLOUD has developed the operation guide for cloud service security and privacy activities to standardize the privacy protection requirements that cloud services must comply with in the product lifecycle. Huawei Cloud builds a privacy protection system based on global privacy protection laws and regulations and best practices widely recognized in the industry to protect privacy and personally identifiable information. Huawei Cloud has established a series of data protection measures to ensure data and information security. To better protect data subjects' rights and protect personal data security. Huawei Cloud implements the basic principles of personal data processing in each phase of personal data processing, specifies the control requirements for the entire lifecycle of personal data processing, and incorporates these requirements into all business activities.
A.5.35	Independent review of information security	The organization’s approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Huawei Cloud has developed the internal audit management process to standardize the internal audit principles, audit management process, and audit frequency. A dedicated audit team performs an internal audit on Huawei Cloud every year to check the running status of the company's internal control system and evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators. Huawei Cloud regularly hires independent third parties to provide external audit and verification services. These evaluators perform regular security assessment and compliance audits or checks. (E.g. SOC,

			ISO standards, PCI DSS audit) to assess the security, integrity, confidentiality, and availability of information and resources for an independent assessment of risk management content/processes.
A.5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	HUAWEI CLOUD has a dedicated audit team to periodically evaluate the compliance and effectiveness of policies, procedures, measures, and indicators. In addition, independent third-party evaluators provide independent assurance by performing periodic security assessments and compliance audits or inspections. (e.g. SOC, ISO standards, PCIDSS audit) To assess the security, integrity, confidentiality, and availability of information and resources to provide an independent assessment of risk management content/processes. HUAWEI CLOUD regularly organizes internal vulnerability scanning on the Huawei cloud platform. HUAWEI CLOUD evaluates and analyzes each vulnerability, formulates and implements a vulnerability fixing solution or workaround, verifies the fixing status after the vulnerability is fixed, and continuously tracks and confirms that the risk is eliminated or mitigated. HUAWEI CLOUD regularly organizes internal penetration tests on the Huawei cloud platform, simulates attacks from malicious sources to understand and evaluate the security of HUAWEI CLOUD, and tracks and rectifys the penetration test results. Penetration test reports and follow-up are verified by internal audits and external certification agencies.
A.5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Huawei Cloud follows the established information security management system, including asset security, access control, cryptography, physical security, operational security, communication security, system secure development, supplier management, information security incident management, and business continuity. Huawei Cloud protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. The cybersecurity management policies and procedures are reviewed at least once a year and updated as needed to reflect changes in business objectives or risk environments by Huawei Cloud. Changes to information security policies and procedures require management approval. At the same time,

			Huawei Cloud has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators, and report the results and recommendations of the investigation to the top management. HUAWEI CLOUD has developed documented information security policies and procedures to guide operations related to information processing and communication facilities. Employees are authorized to view published information security policies and procedures.

5.2.2 A.6 People controls

No.	Control Domain	Control	HUAWEI CLOUD's response
A.6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	If permitted by applicable laws, HUAWEI CLOUD will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Simultaneously, to ensure orderly internal management and reduce the potential impact of personnel management risks on business continuity and security, HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers, including on-boarding security review, on-the-job security training and enablement, on-boarding qualifications management, and off-boarding security review.
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities. Huawei Cloud employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities. For external personnel, HUAWEI CLOUD signs a non-disclosure agreement with them and conducts information security training, including information security responsibilities.

A.6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. HUAWEI CLOUD continues security awareness training for employees during their employment. There is a special information security awareness training program for employees. This training includes but is not limited to, on-the-spot speeches and online video courses. According to the information security awareness training plan, Huawei Cloud continuously provides security awareness training for employees during their on-the-job period to raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations.
A.6.4	Disciplinary process	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	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. 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.
A.6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall	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 security review checklist, which includes the clearance or modification of the resignation account permissions. HUAWEI CLOUD has formulated personnel security

		be defined, enforced and communicated to relevant personnel and other interested parties.	relevant management regulations, requiring employees to transfer their HUAWEI CLOUD assets to the company when they transfer and resign. 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. 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. HUAWEI CLOUD employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities. For external personnel, the contact departments sign non-disclosure agreements with their company based on service requirements.
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	The employment agreement signed between the employee and the company contains confidentiality clauses, which clearly state the employee's cybersecurity responsibilities to ensure that the confidentiality clauses to be followed are confirmed before onboarding. Huawei Cloud employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities.
A.6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	HUAWEI CLOUD employees use unique identity in the internal office network. If the external network needs to be connected to HUAWEI working network, it is necessary to access through VPN. For O&M scenarios, centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in HUAWEI CLOUD data centers. The data center external network operation and maintenance personnel and intranet operation and maintenance personnel centrally manage all local and remote operations of network, server and other equipment, and realize unified access,

			unified authentication, unified authorization, and unified auditing of equipment resource operation management by users. For remote management of HUAWEI CLOUD, whether from the Internet or office network, it is necessary to first access the resource pool bastion host, and then access related resources from a bastion server.
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Huawei Cloud reviews and summarizes the impact and handling processes of security incidents, and informs and reports to the corresponding affected users and regulatory departments as required. Huawei Cloud has developed a complete process for incident management and notification. If an incident occurs on the Huawei Cloud Base Platform, relevant personnel will analyze the impact of the incident according to the process. If the incident has or will have an impact on the cloud service customers, Huawei Cloud will start to notify customers of the incident. The contents of the notice include but are not limited to description of the incident, the cause, impact, measures taken by Huawei Cloud, and measures recommended for customers. HUAWEI CLOUD has established a comprehensive incident notification mechanism for security incidents that affect cloud service customers. A dedicated team will announce major incidents on the official website to ensure that cloud service customers know the occurrence of major incidents and the handling progress of the incidents. For incidents that may affect cloud service customers, HUAWEI CLOUD arranges dedicated customer service personnel to communicate with cloud service customers through the external work order system or the external bulletin platform on the HUAWEI CLOUD official website to protect the rights and interests of cloud service customers. 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. The requirements include that employees should report information security weaknesses they find. For other external partners, HUAWEI CLOUD signed confidentiality agreements with them and

			conducted information security training, which included information security incident reporting responsibilities. HUAWEI CLOUD provides employees with channels and precautions to report information security events. Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services.

5.2.3 A.7 Physical controls

No	Control Domain	Control	HUAWEI CLOUD's response
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Huawei Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures. The Huawei Cloud information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented. Huawei Cloud through access control systems, strictly review and regularly audit user access rights. Huawei Cloud requires visitors to be accompanied by internal personnel throughout the visit, and can only move in general restricted areas. The data center reasonably divides the physical area of the data center (including highly sensitive area) and reasonably arranges the components of the information system in the design, construction and operation, so as to prevent the potential physical and environmental hazards. 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.

A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	The HUAWEI CLOUD information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented. HUAWEI CLOUD through access control systems, strictly review and regularly audit user access rights. HUAWEI CLOUD requires visitors to be accompanied by internal personnel throughout the visit, and can only move in general restricted areas. The data center reasonably divides the physical area of the data center (including highly sensitive area) and reasonably arranges the components of the information system in the design, construction and operation, so as to prevent the potential physical and environmental hazards. 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. The equipment room administrator not only conducts routine security checks, but also audits data center access records irregularly to ensure that unauthorized personnel cannot access the data center.
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Huawei Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures. The Huawei Cloud information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented. The HUAWEI CLOUD information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography

			equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented. 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.
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	The HUAWEI CLOUD information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented.
A.7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	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. 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.
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	The HUAWEI CLOUD information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented. 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.
A.7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	HUAWEI CLOUD has formulated and implemented workplace security management regulations, sets requirements on employees' security responsibilities and behavior, formulates policies and procedures to ensure that unattended workspaces are free of publicly visible sensitive documents. At the same time, security awareness education is carried out through awareness education, publicity activities, and BCG and commitment letter signing.
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	HUAWEI CLOUD has formulated regulations on confidential devices and media management, which specify requirements for device placement, protection, and access and formulate operation processes. Important components of the data center are stored in a dedicated electronic encryption safe in the warehousing system, and the safe is switched on and off by a dedicated person. Any spare components of the data center must be obtained by providing an authorized service ticket and must be registered in the warehousing management system. All physical access equipment and warehousing system materials are regularly counted and tracked by dedicated personnel. The equipment room administrator not only conducts routine security checks, but also audits data center access records irregularly to ensure that unauthorized personnel cannot access the data center.
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	HUAWEI CLOUD has formulated and implemented office computer security management regulations, specifying that office asset users are obligated to ensure the security of the assets they use and are responsible for the usage status. Employees should take working laptops with them or properly store them to ensure the security of HUAWEI information stored on the laptops. Employees will promptly report lost or stolen office computers.
A.7.10	Storage media	Storage media shall be managed through their life	Huawei Cloud has formulated and implemented regulations on mobile media management. All types of mobile media are managed by dedicated

		cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	personnel, approved for borrowing, and formatted after being used. Different security requirements are set for the access and use of personally owned storage media and digital devices to areas with different security levels. Huawei Cloud requires storage media to be stored in a controlled access area or in a locked cabinet. When a storage media enters or exits a controlled area, the detailed information from outbound to inbound must be reconciled and tracked in a closed-loop manner. All types of mobile media shall be managed by dedicated personnel. Approval is required for borrowing and must be formatted after use. Personal storage media and digital devices are not allowed into areas with special confidentiality requirements. Huawei Cloud requires that storage media containing Huawei confidential information must be marked. Confidential data shall be marked or labeled according to the data security level, and the security level shall be stated. Labels must be attached to the exterior of media in transit or facilities authorized to store the media, and to the exterior of locked containers used for transporter media. Huawei Cloud has formulated and implemented relevant media management regulations. The storage media for storing confidential information or backups must be encrypted, and should be stored in controlled access areas to prevent unauthorized access and use, to ensure the confidentiality and integrity of data on storage media. Huawei Cloud has formulated and implemented relevant media management regulations, in which the media are cleared and scrapped according to the classification. Huawei Cloud achieves data cleaning, disk demagnetization through a variety of ways, and records the destruction operation. Dedicated personnel manage devices that contain storage media on Huawei Cloud. After the devices are used, dedicated personnel format the devices. When a storage media that stores HUAWEI's confidential information is scrapped, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting.
A.7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other	HUAWEI CLOUD strictly controls the electrical and fire safety. HUAWEI CLOUD data centers employ a multi-level safety assurance solution to make 24/7 service availability and continuity. Daily electricity consumption at data centers relies on dual power supply from different power

		disruptions caused by failures in supporting utilities.	substations. Data centers are equipped with diesel generators, which are run in the event of power outage, and also Uninterruptible Power Supply (UPS), which provides temporary power as a backup. HUAWEI CLOUD data centers comply with Level-1 design and use Class-A fireproof materials for their construction in compliance with country-specific fire control regulations. Flame retardant and fire-resistant cables are used in pipelines and troughs, alongside power leakage detection devices. Automatic fire alarm and fire extinguishing system is deployed to quickly and accurately detect and report fires. Automatic alarm system links with power supply, monitoring, and ventilation systems such that the fire extinguishing system can activate itself even when unattended, autonomously keeping fires under control.
A.7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	HUAWEI CLOUD data centers avoid strong electromagnetic interference during site selection. During the construction of HUAWEI CLOUD data centers, secure conduits and anti-tamper hardware must be used for network cabling and external devices. When communication equipment, such as fiber optic cables, passes through open access areas, pipes and bridges are made of metal, covered with protective cables, laid in pipes or trunkings, and equipped with leakage detection devices.
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	For data center maintenance, HUAWEI CLOUD has established regulations and processes related to data center O&M management, including specific device control measures and routine maintenance plans. Huawei Cloud has formulated asset management procedures, which specify the classification and grading methods of information assets.
A.7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Dedicated personnel manage devices that contain storage media on Huawei Cloud. After the devices are used, dedicated personnel format the devices. When a storage media that stores HUAWEI's confidential information is scrapped, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting. When a physical disk needs to be decommissioned, Huawei Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, Huawei Cloud adheres industry standard practices and

			keeps a complete data deletion activity log for chain of custody and audit purposes.

5.2.4 A.8 Technological controls

No	Control Domain	Control	HUAWEI CLOUD's response
A.8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	HUAWEI CLOUD has formulated regulations on mobile device management to implement unified management of mobile computing devices. The rules for using mobile devices, responsibilities, authority requirements, and security requirements for mobile devices management, network access requirements and violation penalties are stipulated and implemented. For laptops, 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. HUAWEI CLOUD has formulated and implemented workplace security management regulations, sets requirements on employees' security responsibilities and behaviors, formulates policies and procedures, and implements access control to ensure proper protection of unattended user devices.
A.8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Huawei Cloud has defined management requirements for privileged accounts. Privileged accounts are classified and comply with management requirements during the creation, recycling, authorization, use, and deregistration of privileged accounts. The privileged account management system binds functional and technical accounts for daily and emergency O&M to O&M teams or individuals. Privileged or contingency accounts are granted to employees only when required by their duties. All requests for privileged or emergency accounts are reviewed and approved at multiple levels. Huawei Cloud will only log in to the tenant console or resource instance to assist the customer in maintenance after obtaining the customer's authorization. Huawei Cloud administrators must pass two-factor authentication in order to access the management plane through bastion hosts, and enables comprehensive logging and centralized log management of all administrator-level O&M activities to ensure that all operations on the target host can be traced to any O&M personnel. The privileged account management system binds functional and technical accounts for daily and emergency O&M to O&M teams or

			individuals. Privileged accounts of assets such as OS hosts, network devices, and security devices are centrally managed by the privileged account management system and their passwords are automatically changed. When using privileged accounts, O&M personnel need to submit service tickets and perform routine audits to ensure the security of privileged accounts.
A.8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimized permission assignment and strict behavior audit ensure that unauthorized access is not performed. Huawei Cloud implements RBAC permission management based on different service dimensions and responsibilities of the same service. The login permission is classified into the following types: core network, access network, security devices, service systems, database systems, hardware maintenance, and monitoring maintenance. Any O&M personnel is restricted to access only devices within the administrative scope of his/her role and is not granted permissions to access other devices.
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Huawei Cloud uses the internal DevOps platform to implement automatic building, testing, and rollout during the application security development lifecycle, preventing software from being tampered with during transmission in the environment. The Huawei Cloud information security environment is managed by partitions. Unauthorized network connection between the test environment and production environment are prohibited to avoid security risks in the production environment due to the intrusion of the test environment. It's not allowed to download source code, access source code from outside the company, or transfer source code through basic office applications. Transfer of source code from the corporate information security environment to the outside of the company must be approved and controlled.
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific	Huawei Cloud emphasizes that security risks of employee cloud service accounts are controllable. Strong passwords are strictly required. Account permissions are regularly reviewed. Privileged accounts are strictly managed and reclaimed. Huawei Cloud IAM is used to manage access and supports multi-factor authentication for login verification and operation protection. Employees need to use multi-factor authentication to determine their identity each time they log in. Huawei Cloud has

		policy on access control.	set a maximum of five login attempts to prevent unlimited login attempts using invalid passwords. Successful and failed login attempts of the system, middleware, and network infrastructure are recorded in logs. Illegal logins or attempted logins are reported through regular log review and log alarms.
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	HUAWEI CLOUD has formulated capacity management regulations to manage HUAWEI CLOUD capacity in a unified manner and improve the availability of HUAWEI CLOUD resources. Identify the effectiveness of resource requirements and manage the resource capacity based on the daily capacity level of HUAWEI CLOUD to guide the development of resource capacity expansion and reduction solutions. In addition, HUAWEI CLOUD has formulated the principles of transparent management, clear authorization, and efficient operation, and specified authorization rules for organizations at all levels in data center construction and capacity management decision-making. HUAWEI CLOUD monitors the capacity allocation of physical hosts based on the capacity monitoring platform. The capacity monitoring team configures alarm policies on the IoT platform so that when an exception occurs, the IoT platform can automatically send alarm emails to related product O&M personnel or capacity managers for follow-up. HUAWEI CLOUD has established a weekly meeting mechanism. The responsible department reviews the resource requirements in the current week during the weekly meeting. After the review is passed, capacity expansion measures will be taken accordingly. In addition, the HUAWEI CLOUD Infrastructure Engineering Dept analyzes the capacity configuration status of the service every month based on the actual service operation status, analyzes and estimates the potential capacity requirements of the next month, and records the analysis and estimation results in the monthly analysis report. HUAWEI CLOUD has established a formal capacity expansion review process. Business departments need to submit applications through the unified resource management platform and obtain approval from the planning committee before performing resource expansion.
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by	At the physical host level, antivirus software is deployed to achieve defense against malware attacks. Unified terminal protection software is deployed on terminal devices, which has the ability to protect terminal devices from malware attacks, and periodically updates the malware

		appropriate user awareness.	protection mechanism. Huawei Cloud configures settings in the backend system to ensure that employees cannot uninstall or disable the data. Huawei Cloud uses IPS intrusion prevention system, Web Application Firewall (WAF), 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 functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web tamper protection. Huawei Cloud provides security awareness education for employees during their on-the-job years. There is a dedicated information security awareness training program, including malware prevention.
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	HUAWEI CLOUD has established a security vulnerability management process. Vulnerability administrators and related security roles are responsible for vulnerability assessment. In addition, HUAWEI CLOUD specifies vulnerability grading, responsibility assignment, and vulnerability handling requirements for periodic installation of key security patches to reduce vulnerability risks. In addition, HUAWEI CLOUD has set up a dedicated vulnerability response team to evaluate and analyze the cause and threat level of vulnerabilities in a timely manner, formulate remedial measures, and evaluate the feasibility and effectiveness of remedial solutions. HUAWEI CLOUD has established a vulnerability scanning mechanism to periodically scan assets (including applications, IP addresses, and accounts) on the cloud platform. Follow the vulnerability management process to track the vulnerabilities detected during scanning. Open-source and third-party scanning tools used by HUAWEI CLOUD are obtained from official channels. Commercial tools must be authorized. HUAWEI CLOUD regularly organizes internal penetration tests on the Huawei cloud platform, simulates attacks from malicious sources to

			understand and evaluate the security of HUAWEI CLOUD, and tracks and rectifys the penetration test results. Penetration test reports and follow-up are verified by internal audits and external certification bodies.
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Huawei Cloud establishes unified baseline configuration standards for server operating systems, database management systems, and network devices that support service operation to implement unified management of service baseline configurations, specify security configuration requirements for systems/components in the production environment, and ensure effective execution and continuous improvement of security configurations. 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 and establish an internal technical standard and specification library that contains information security baselines of infrastructure components. Systems or components entering the Huawei Cloud production environment are performed self-inspection by each business delivery team based on the security configuration standards. If the product acceptance team finds that it does not meet the security configuration standards during acceptance, the product acceptance team must complete rectification before entering the production environment. All products must be checked by the security engineering laboratory in accordance with the corresponding security configuration standards before releasing, and the configuration changes of products must follow the change management process.
A.8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	When customer data is destroyed on Huawei Cloud, the data is deleted, along with all its copies. After a user confirms data deletion, Huawei Cloud fiàâì deletes the indexing between the user and the data. Then, Huawei Cloud zeroes out the storage resources involved, such as memory and block storage space. This ensures that deleted data and related information cannot be restored or recovered if those storage resources are later reallocated to other users. Huawei Cloud also follows comprehensive storage media disposal procedures based on industry standards to ensure data security at the end of the data center media lifecycle. In compliance with the NIST Special Publication 800-88 guideline, data on the storage media that needs to be reused is overwritten by random numbers, or deleted after encryption. Storage

			media that does not need to be reused is degaussed or physically destroyed.
A.8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, data transmission channel approval, and auditing. Huawei Cloud strictly controls the flow of unanonymized data into the test environment to prevent production data or unanonymized production data being used for testing. Data cleaning is required after use. Before the production data is used in the test environment, the authentication credential data (such as passwords and keys) and confidential business data (such as pricing information) need to be removed, and the personal data need to be anonymized. Unauthorized network connection between the test environment and production environment are prohibited to avoid security risks in the production environment due to the intrusion of the test environment.
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Huawei Cloud has formulated regulations for managing storage media and devices in and out of the equipment room. Storage media and devices must be registered and authorized before entering or leaving the equipment room. Data leakage prevention management is implemented when physical storage media enters and exits the equipment room, and data erasing and scrapping processes are specified to reduce possible data leakage losses. If sensitive personal data is involved in the customer's business data, the cloud service encrypts the data by default. Data transmitted between untrusted networks is encrypted. Secure encryption channels (e.g. HTTPS) are used during information transmission, and stored static data is encrypted and protected by secure encryption algorithms to ensure the confidentiality of data in different states. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.
A.8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Huawei Cloud has formulated and implemented backup and redundancy policies, including development and test environment, code document version management, backup and redundancy of the production system, tool software and security equipment. Huawei Cloud has formulated data backup specifications to standardize the data backup format, backup time, backup content, and policy. In addition, Huawei Cloud standardizes the formulation of service recovery policies to ensure that services can be recovered to an acceptable level within the

			recovery time objective. Huawei Cloud has established a node data backup mechanism. The eBackup system backs up node data, if the backup fails, the eBackup system automatically sends an email to the backup administrator for follow-up. Huawei Cloud can replicate and store user data on multiple nodes in a data center. Once a single node is faulty, user data will not be lost and the system can automatically detect and recover. Data centers in different availability zones in a region are interconnected through high-speed optical fibers, meeting basic requirements for cross- availability zone data replication. Users can select data replication services based on service requirements. In addition, storage and database services provided by Huawei Cloud are highly reliable. For example, EVS uses the multi-copy data redundancy protection mechanism and the synchronous write and read repair mechanism to ensure data consistency. If a hardware fault is detected, EVS automatically rectifies the fault in the background and quickly rebuilds data. The data durability reaches 99.999999999%. OBS provides highly reliable storage. With redundant node design and highly reliable networks connecting service nodes, it offers 99.995% availability, fully meeting the requirements for high availability of object storage services. In addition, by using automated recovery technology that provides data redundancy and ensures consistency, OBS offers data durability of 99.999999999999%. The RDS uses the hot standby architecture. If a fault occurs, the system automatically switches services to the standby node within 1 minute. Data is automatically backed up every day and uploaded to OBS buckets. Backup files are stored for 732 days. One-click restoration is supported.
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most

			outage scenarios (including natural disasters and system failures).
A.8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.	HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. HUAWEI CLOUD also has a dedicated internal audit department that performs periodic audits on O&M activities.
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	For the log analysis platform that stores security logs in a centralized manner, the system administrator periodically checks the collection status and storage status to ensure the availability of security logs. HUAWEI CLOUD log analysis platform collects security logs of related O&M systems, servers, and network devices, and presets abnormal operation rules on the platform to identify abnormal operations, generate alarms, and send the alarms to emergency response personnel for analysis and handling. Abnormal alarms are monitored and recorded on the event analysis and handling platform in real time. In addition, HUAWEI CLOUD has a 7 x 24 professional security incident response team and expert resource pool to handle alarms in real time according to the security incident emergency response process.
A.8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Huawei Cloud uses the standard NTP4.2.8 protocol to synchronize time in the system in a centralized manner to synchronize the clock time between the communication equipment and the communication network, so as to ensure the consistency of the time of each network element in the system.
A.8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	HUAWEI CLOUD divides the data center into multiple security areas based on business functions and network security risks, realizing physical and logical control. HUAWEI CLOUD O&M personnel must first log onto the Virtual Private Network (VPN) to connect to this security zone and then log onto managed nodes through bastion hosts. HUAWEI CLOUD administrator-level personnel can access O&M interfaces of all security zones from this security

			zone. This security zone does not expose its interfaces to any other security zone. The O&M management platform assigns permissions through permission management groups. The application for joining a permission management group must be approved by the administrator of the corresponding permission management group. In addition, bastion hosts are granted permission by service domain groups. The application for adding a service domain group must be approved by the administrator of the global O&M center. After the administrator approves the application, bastion hosts automatically create a new service domain group. When an employee applies for joining a bastion host service domain group, the administrator of the service domain approves the application. After the administrator approves the application, the bastion host system adds the employee to the specified service domain group.
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	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, software installation, and software exit. HUAWEI CLOUD has developed and implemented desktop terminal service software standard. Office computers use only the standard operating systems and software defined in the standard.
A.8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Every HUAWEI CLOUD data center has numerous nodes and complex functional zones. To simplify its network security design, prevent the propagation of network attacks in HUAWEI CLOUD, and minimize the potential impact of attacks, HUAWEI CLOUD defines both security zones and service planes, and implements a network segregation strategy in HUAWEI CLOUD by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. HUAWEI CLOUD always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, HUAWEI CLOUD has adopted a set of network security mechanisms to enforce stringent

			controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks.
A.8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	HUAWEI CLOUD defines the security mechanism, service level agreement (SLA), and management requirements for network services in the agreements signed with network service providers.
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Based on business functions and network security risks, the HUAWEI CLOUD data center network is mapped into different security zones to achieve network isolation using both physical and logical controls, which boosts the network immunity and fault tolerance1 in HUAWEI CLOUD in response to attacks from external threat actors and internal threats. The following list describes the five key security zones: DMZ zone, Public services zone, Point of Delivery (POD), Object - Based Storage (OBS), and Operations Management (OM). In addition to the above-mentioned security zoning for every HUAWEI CLOUD data center's network, distinct security levels within different security zones are also defined for HUAWEI CLOUD. Attack surfaces and security risks are determined based on different business functions. For example, security zones that are directly exposed to the Internet have the highest security risks, whereas the O&M zone that exposes no interface to the Internet therefore has a much smaller attack surface, lower security risks, and less challenging to manage.
A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Huawei Cloud personnel follow Huawei's security control requirements for Email systems, mobile mail usage, and network access and usage. Huawei Cloud uses technical means approved by Huawei, such as deploying anti-virus programs, monitoring and filtering emails at the mail gateway, and intercepting virus mail and spam. In addition, Huawei Cloud is prohibited from enabling network services such as WWW, FTP, DNS, and dynamic routing on the office network without permission or providing network proxy services on the office network. It also prohibits shared directories for which all users have access rights. When an employee accesses the Huawei Cloud office

			network through the Internet, the employee must use the virtual private network (VPN) that supports registered authentication devices and two-factor authentication with account password. HUAWEI CLOUD implements permission control through IT systems, which clarify that users are prohibited from logging in to their private email addresses (other than Huawei Email) through Proxy without authorization, and it is prohibited to transmit Huawei information outside Huawei's office network through the network. It is also forbidden to use any means to bypass proxy restrictions to transmit data outside the company or access unauthorized websites. It also prohibits shared directories for which all users have access rights.
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Huawei Cloud formulates and implements cryptographic algorithm application specifications. This document describes how to select secure encryption algorithms and the rules for using secure encryption algorithms. It also provides guidance on the correct use of cryptographic algorithms with application examples. Huawei Cloud uses the AES encryption method widely used in the industry to encrypt data on the platform, and uses the high-version TLS encryption protocol to secure data during the transmission processes, ensuring data confidentiality in different states. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks. Huawei Cloud implements the cryptographic algorithm application specification maintained by Huawei Cyber Security Competence Center, which contains the standardized information list of common cryptographic algorithms and solutions. This list has been referenced to widely used standards and best practices in the industry to guide products to correctly select and use cryptographic algorithms. Huawei Cloud has formulated and implemented key management security specifications to manage security in each phase of the key lifecycle， and specifies security management requirements for key generation, transmission, use, storage, update, backup and recovery, and destruction. All Huawei Cloud business domain should comply with key management security specifications and implement security controls on key generation, key storage, key distribution, key update and key destruction to prevent key leakage and damage. In addition, Huawei Cloud uses Key Management Service (KMS) to manage the master keys of RDS and OBS users.

			RDS and OBS invoke internal interfaces of KMS to request the master keys for encryption and decryption.
A.8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	HUAWEI CLOUD implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, etc. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.
A.8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	HUAWEI CLOUD implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, etc. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly

			automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.
A.8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	HUAWEI CLOUD implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, etc. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat

			mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Huawei Cloud strictly complies with the secure coding specifications released by Huawei. Before they are on boarded, Huawei Cloud service development and test personnel are all required to learn corresponding specifications and prove they have learned these by-passing examinations on them. In addition, we 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. Huawei Cloud uses the internal DevOps platform to implement automatic building, testing, and rollout during the application security development lifecycle, preventing software from being tampered with during transmission in the environment.
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	All cloud services pass multiple security tests before release, 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. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. In addition, Huawei Cloud leverages its in-depth understanding of customers' security requirements and industry standards and develops matching security test tools. One such tool is SecureCAT, which can be used to check security configurations of mainstream OS and database systems. Once integrated, such security capabilities, controls and tools can be used and reused many times. Huawei Cloud has established formal internal testing and acceptance measures to ensure that only appropriate and authorized changes are released to the production environment.

A.8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	HUAWEI CLOUD has specified requirements on R&D outsourcing management, and incorporates the supervision of outsourced personnel and outsourced projects into the daily responsibilities of employees and projects. 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.
A.8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Huawei Cloud standardizes general information security management requirements for R&D environments and information security management during environment planning, construction, use, maintenance, and cancellation. In addition, Huawei Cloud standardizes the deployment and release processes of products/services that use the DevOps development mode, which regulates the requirements for environment isolation. Software products that pass the verification test need to be deployed to the production environment in batches in accordance with business requirements and technical requirements, and release policy to ensure effective control of changes to the production environment and improve the stability of the production environment. Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, data transmission channel approval, and auditing. Huawei Cloud strictly controls the flow of unanonymized data into the test environment to prevent production data or unanonymized production data being used for testing. Data cleaning is required after use.
A.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Huawei Cloud has developed a standard change management process. Changes to elements in the production environment need to be managed in an orderly manner. After a change application is generated, the change manager determines the change level and submits it to the Huawei Cloud Change Committee. After the application passes the review, the change can be implemented in production environment as planned. 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.
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, data transmission channel approval, and auditing. Huawei Cloud strictly controls the flow of unanonymized data into the test environment to prevent production data or unanonymized production data being used for testing. Data cleaning is required after use. Before the production data is used in the test environment, the authentication credential data (such as passwords and keys) and confidential business data (such as pricing information) need to be removed, and the personal data need to be anonymized. Unauthorized network connection between the test environment and production environment are prohibited to avoid security risks in the production environment due to the intrusion of the test environment.
A.8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	HUAWEI CLOUD has developed and implemented regulations on penetration testing and vulnerability scanning, which define risk mitigation policies. In terms of time selection, the penetration test and scanning activities that have great impact on the system must avoid peak hours, major activity dates, and emergency assurance periods. At the same time, a hierarchical strategy is formulated, which includes not performing large-scale concurrent scanning on targets, performing batch and time-based scanning and controlling the generated data traffic. During the scanning, servers with relatively unimportant services are selected first, and other systems are scanned if there is no risk.

6 HUWAEI CLOUD Helping Customers Respond to ISO 27001 Requirements

HUAWEI CLOUD has passed ISO 27001 certification and provides secure and reliable cloud services for customers. However, this does not mean that customers who use HUAWEI CLOUD services meet the control requirements of ISO 27001 by default. If the customer wishes to be ISO 27001 certified, it should establish, implement, maintain and continuously improve its own information security management system in accordance with ISO 27001 guidelines and best practices, and contact a third-party independent certify unit for evaluation.

The establishment of ISMS needs to start from two aspects: management and technology. At the management level, customers should develop information security policies and procedures that meet their own needs and meet the requirements of ISO 27001. At the technical level, products and services provided by HUAWEI CLOUD can help customers in some control domains and help them solve problems encountered when building their own information security management system.

For details about the products that can help achieve the objectives of control domains in ISO 27001, please find the following table. For details about the products, please refer to the **Product Page** on the HUAWEI CLOUD official website. The following sections describe how some of HUAWEI CLOUD's main products help customers achieve the control objectives in the ISO 27001:2022 control domain.

ISO 2700 Control	Products that Help in Achieving the Objectives	Control Requirements that Help in Achieving the Objectives
A.5	**Data Security Center (DSC)**、**Host Security Service (HSS)**、**Object Storage Service (OBS)**	A5.9、A5.12、A5.13
	Virtual Private Cloud (VPC)、**Virtual Private Network (VPN)**、**Cloud Certificate Manager (CCM)**、**Direct Connect (DC)**、**Cloud Connect (CC)**	A5.14
	Identify and Access Management (IAM)	A5.15、A5.16、A5.17、A5.18
	Cloud Eye Service (CES)、 **Application Operations**	A5.19、A5.20、

	Management (AOM)	A5.21、A5.22、A5.23
	Managed Threat Detection (MTD)	A5.24、A5.25、A5.26、A5.27
	Cloud Backup and Recovery (CBR)、 **Cloud Server Backup (CSBS)**、 **Storage Disaster Recovery Service (SDRS)**	A5.28、A5.29、A5.30
A.6	**Managed Threat Detection (MTD)**	A6.8
A.8	**Identify and Access Management (IAM)**、 **Cloud Bastion Host (CBH)**	A8.2、A8.5
	Cloud Eye Service (CES)	A8.6
	Web Application Firewall (WAF)、**Host Security Service (HSS)**	A8.7
	Database Security Service (DBSS)、**Data Security Center (DSC)**	A8.11
	Data Encryption Workshop (DEW)、**Elastic Volume Service (EVS)**、**Image Management Service (IMS)**、**Object Storage Service (OBS)**	A8.12
	Cloud Backup and Recovery (CBR)、 **Cloud Server Backup (CSBS)**	A8.13
	Elastic Load Balance (ELB)	A8.14
	Cloud Eye Service (CES)、**Log Tank Service (LTS)**、**Cloud Trace Service (CTS)**	A8.15、A8.16
	Cloud Bastion Host (CBH)	A8.18
	Virtual Private Cloud (VPC)、**Virtual Private Network (VPN)**、**Anti-DDoS Service (AAD)**	A8.20、A8.21、A8.22
	Web Application Firewall (WAF)、**Host Security Service (HSS)**	A8.23
	Data Encryption Workshop (DEW)	A8.24
	CodeArts、**CodeArts TestPlan**、**API GatewayAPIG**、**CodeArts PerfTest**、**CodeArts Check**	A8.25、A8.26、A8.27、A8.28、A8.29、A8.31、A8.32

6.1 Product Functions

- **Data Security Center**

HUAWEI CLOUD **Data Security Center (DSC)** is a new-generation cloud-native data security platform that provides customers with basic data security capabilities, such as data classification, data security risk identification, data watermark source tracing, and data anonymization. In addition, the data security overview integrates the status of each phase of the data security lifecycle to present the overall data security situation on the cloud.

- **Host Security Service**

Customers can also use **Host Security Service (HSS)** to comprehensively identify and manage information assets on hosts, monitor risks on hosts in real time, prevent unauthorized intrusions, and build a server security system to reduce major security risks faced by servers. Customers can view and manage the protection status and security risks of all hosts in the same region on the GUI provided by. For host security protection, **Host Security Service (HSS)** of HUAWEI CLOUD implements comprehensive security assessment on the host system. After the assessment, HSS displays the risks of accounts, ports, software vulnerabilities, and weak passwords in the existing system, prompting customers to perform security hardening. This feature eliminates security risks and improves the overall security of the host. HSS also provides the intrusion detection function. When an event such as brute force cracking of accounts, process exceptions, and abnormal logins is detected, an alarm is generated quickly. Customers can learn about alarm events through event management, helping them detect security threats in assets in a timely manner and learn the security status of assets, use intrusion detection to detect and prevent intrusions into the network.

- **Object Storage Service**

Object Storage Service (OBS) stores unstructured data in customers' information assets. OBS supports lifecycle management of storage objects and helps customers manage their information assets. In addition, multiple security protections in OBS, such as SSL transmission encryption, server-side encryption, and identity authentication, can protect stored information.

- **Virtual Private Cloud**

Virtual Private Cloud (VPC) provided by HUAWEI CLOUD enables tenants to build an isolated and private virtual network environment, isolate tenants during smooth access, and flexibly configure interconnection and interworking between VPCs. Customers can fully control the construction and configuration of their virtual networks, including subservices such as IP address ranges, subnets, and security groups in the VPC. By configuring network ACLs and security group rules, they can strictly control network traffic to and from subnets and VMs. Meet customers' fine-grained network isolation requirements. Customers can use VPC to divide network areas and establish isolated production and test environments on the cloud.

- **Virtual Private Network**

In scenarios where existing data centers need to be expanded to HUAWEI CLOUD, customers can use **Virtual Private Network (VPN)**. This service can be used to establish secure and encrypted communication tunnels between local data centers and VPC provided by HUAWEI CLOUD. Customers can use resources such as cloud servers and block storage on the cloud platform to transfer applications to the cloud, start additional web servers, and increase network computing capacity. Implement a hybrid cloud architecture for enterprises.

- **Direct Connect**

Direct Connect allows tenants to establish stable, high-speed, low-latency, secure dedicated network connections between their local data center and a VPC on Huawei Cloud. It leverages Huawei Cloud services and existing IT facilities to build a flexible, scalable hybrid cloud computing environment. These connections can be used to interconnect Huawei Cloud with tenants' data centers, offices, and hosting centers with lower latency. Compared with a public

Internet connection, Direct Connect offers a faster, more secure network experience for tenants.

- **Cloud Connect**

Cloud Connect (CC) enables users to quickly build high-speed, high-quality, and stable networks between VPCs across regions and between VPCs on the cloud and multiple data centers off the cloud, helping users build a global cloud network with enterprise-level scale and communication capabilities. By creating a cloud connection, you can load network instances in different regions that need to communicate with each other to the created cloud connection instance. The network instance can be a VPC instance created by the user or a VGW instance created by the user for local data center access. It can also be a VPC instance that can be loaded by another user. You can configure the inter-domain bandwidth between the network instances that need to communicate with each other to quickly provide global network interconnection services for you.

- **Cloud Certificate Manager**

Cloud Certificate Manager (CCM) of HUAWEI CLOUD provides customers with one-stop certificate lifecycle management, implementing trusted identity authentication and secure data transmission for websites. CCM includes the SSL Certificate Manager (SCM) and Private Certificate Authority (PCA) services. The platform cooperates with world-renowned digital certificate authority to provide users with the SSL certificate purchase function. Customers can also upload local external SSL certificates to the IoT platform to centrally manage internal and external SSL certificates. After deploying the service, customers can replace the HTTP protocol used by the service with the HTTPS protocol to eliminate security risks of the HTTP protocol. This service can be used for website authentication, application authentication, and data transmission protection. The platform allow users to set up a complete CA hierarchy and use it to issue and manage private certificates for the organization.

- **Identify and Access Management**

Identity and Access Management (IAM) provided by HUAWEI CLOUD. Provides user account management services suitable for enterprise-level organizations and assigns different resources and operation rights to users. After using the access key to obtain IAM-based authentication, users can call APIs to access HUAWEI CLOUD resources. IAM enables hierarchical and fine-grained authorization to ensure that different users of the same customer can use cloud resources effectively, preventing the entire cloud service from being unavailable due to misoperation of a single user, and ensuring service continuity.

IAM supports user group-based permission management, allows users to set password policies, password change periods, login policies, account locking policies, account disabling policies, and session timeout policies that meet customers' status, and provides IP-based ACLs. IAM also provides and enables multi-factor authentication by default to enhance account security. If a customer has a secure and reliable external identity authentication service (such as LDAP or Kerberos) to authenticate users and the external service supports SAML 2.0, users can use SAML to log in to the HUAWEI CLOUD service console or access cloud resources through APIs.

- **Cloud Eye Service**

Customers can use **Cloud Eye Service (CES)** provided by HUAWEI CLOUD to monitor utilization of ECS resources and network bandwidth in a multi-dimensional manner. CES reports tenant-defined alarm rules using open APIs, SDKs, and Agents, and send notifications through emails and SMS messages to ensure that customers know service running status in a real time.

- **Application Operations Management**

Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform that enables customers to monitor their applications and track performance and resource changes in real time. It provides a unified data view of events, logs, and metrics, so that customers can optimize resources and fine tune application performance.

- **Managed Threat Detection**

Managed Threat Detection (MTD) continuously checks source IP addresses and domain names in cloud service logs and alert you to potential malicious activities and unauthorized behaviors. MTD can monitor logs of IAM, DNS, CTS, and OBS, all of which are global services in your account. Powered by an AI engine, threat intelligence, and detection policies, MTD intelligently examines access behavior in logs of cloud services to detect threats, generate alarms, and provide remediation. With MTD, you can respond to alarms, handle potential threats, and harden service security in a timely manner to prevent major losses such as information leakage, keeping your accounts and service secure and stable.

- **Cloud Backup and Recovery**

Customers can use **Cloud Backup and Recovery (CBR)** to back up **Elastic Volume Service (EVS)**, **Elastic Cloud Server (ECS)** and **Bare Metal Server (BMS)**. CBR supports backup based on the consistency snapshot technology to restore data for cloud server and EVS using backups. In addition, CBR supports the synchronization of backups in the offline backup software BCManager and the integrity verification of backups.

For example, customers can use **Cloud Backup and Recovery (CBR)** to back up cloud servers, disks, file services, off-cloud files, and VMware virtual environments. Data can be restored to any backup point when data is unavailable due to virus intrusion, accidental deletion, or software/hardware fault.

- **Cloud Server Backup**

If customers want to create online backups, they can use **Cloud Server Backup Service (CSBS)**, it creates consistent online backups for EVS disks on ECSs. If there is a virus intrusion, accidental deletion, or software/hardware fault, data can be restored to any backup point. CSBS works based on the consistency snapshot technology to provide backup service for ECS and BMS, it supports to restore data using data backups, ensuring the security and correctness of user data to the maximum extent and ensuring business security.

- **Storage Disaster Recovery Service**

To meet organizations' requirements for information security and information security management continuity in the event of disasters, **Storage Disaster Recovery Service (SDRS)** provides disaster recovery (DR) protections for ECS, EVS and **Dedicated Distributed Storage Service (DSS)**. SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide high data reliability and service continuity for users. SDRS protects service applications by replicating the server data and configurations to a DR site. It allows service applications to start at the DR site in the event that servers at the production site stop. This improves service availability and continuity.

- **Cloud Bastion Host**

Host Bastion Host (CBH) is a unified 4A security management and control platform of HUAWEI CLOUD. It helps customers implement centralized account, authorization, authentication, and audit management. CBH provides cloud computing security management and control systems and components. It integrates functions such as single sign-on (SSO), unified asset management, multi-terminal access protocols, file transfer, and session collaboration. Customers can use the unified O&M login portal to centrally manage and audit cloud resources such as servers, cloud hosts, databases, and application systems. CBH can be used to implement access control and unified operation log audit in scenarios such as

customer employees logging in to the company system, O&M personnel accessing O&M network areas, employees remotely accessing related resources from external networks, and administrators accessing the management platform, ensuring that networks and network services are accessed only by authorized users.

- **Web Application Firewall**

Customers can deploy **Web Application Firewall (WAF)** to detect and protect website service traffic from multiple dimensions. With deep machine learning, can intelligently identify malicious request characteristics and defend against unknown threats, and detect HTTP(S) requests. Identifies and blocks SQL injection, cross-site scripting attacks, web page uploading, command/code injection, file inclusion, sensitive file access, third-party application vulnerability attacks, CC attacks, malicious crawler scanning, and cross-site request forgery, preventing websites from being maliciously attacked and invaded by hackers, secure and stable web services.

- **Data Encryption Workshop**

Customers can use the **Data Encryption Workshop (DEW)** provided by HUAWEI CLOUD to implement dedicated encryption, key management, and key pair management. DEW supports key creation, authorization, automatic rotation, and key hardware protection. Customers can select the required key management mechanism as required.

HUAWEI CLOUD provides cloud Hardware Security Module (HSM) of different vendors, specifications (such as standard encryption algorithms and Chinese national cryptographic algorithm), and strengths to meet customers' requirements. HSMs are deployed in a two-node cluster to ensure high reliability and availability.

Customers can use Key Management Service (KMS) to bind keys to identifiable owners. All keys in KMS are generated by the hardware true random number generator of the HSM to ensure the randomness of keys. The root key of KMS is stored in the HSM to ensure that the root key is not disclosed. KMS hosts use the standard encrypted transmission mode to establish secure communication links with KMS nodes to ensure secure transmission of KMS-related data between nodes. KMS implements RBAC access control based on roles in IAM. A user can operate the master key stored in KMS only after being authenticated by and KMS and having the key operation permission. Users with only the read-only permission can query only the master key information but cannot perform operations on the master key. KMS isolates CMKs from customers. Each tenant can access and manage only its own CMKs, but cannot operate the CMKs of other tenants. In addition, the system administrator has only device management rights and does not have any access to the master key.

- **Elastic Volume Service、Image Management Service**

Customers can use the snapshot function of **Elastic Volume Service (EVS)** to restore data to the snapshot point in time when data is lost. HUAWEI CLOUD also provides **Image Management Service (IMS)**. Customers can use to back up cloud server instances and use the backup images to restore cloud server instances when the software environment of the instances is faulty. **Cloud Server Backup Service (CSBS)** can create consistent online backups for multiple EVS disks under a cloud server, ensuring data security and reliability and reducing the risk of unauthorized data tampering. **Object Storage Service (OBS)** supports multiple data storage scenarios, customers can also use it for enterprise data backup and archiving.

- **Elastic Load Balance (ELB)**

Customers can use Huawei Cloud **Elastic Load Balance (ELB)**_which automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of

application systems to provide service and enhancing the fault tolerance of application programs.

- **Log Tank Service**

Log Tank Service (LTS) on HUAWEI CLOUD collects, queries, and stores logs in real time. Its records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. With CES, customers can monitor user login logs in real time. If malicious logins occur, an alarm is generated and requests from the IP address are rejected. In addition, LTS and **Database Security Service (DBSS)** can record and save system component logs for customers to audit logs.

- **Cloud Trace Service**

Cloud Trace Service (CTS) of HUAWEI CLOUD records operations performed by users using cloud accounts to log in to the management console in real time. Customers can purchase **Object Storage Service (OBS)** of different specifications to back up logs based on the log retention period.

- **Anti-DDoS Service**

To ensure a secure network protection system, customers can use network technologies and network devices to divide security domains and use a series of security services provided by HUAWEI CLOUD to improve network border protection capabilities. For example, **Anti-DDoS Service (AAD)** provides Cloud Native Anti-DDoS (CNAD) Basic for refined protection against network-layer and application-layer DDoS attacks. Customers can set traffic threshold parameters based on service application types and view the attack and defense status using the real-time alarm function. Customers can use the Anti-DDoS Service (AAD) of HUAWEI CLOUD to detect and clean large-traffic attacks.

- **CodeArts、CodeArts TestPlan**

CodeArts is a one-stop cloud DevOps platform provided by HUAWEI CLOUD for developers. It helps customers perform project management, code hosting, pipeline, code check, compilation and building, deployment, testing, and release on the cloud. It also enables developers to quickly and easily develop in the cloud. By using open APIs and call examples provided by CodeArts, customers can manage projects, work items, members, code repositories, and pipelines. **CodeArts TestPlan**, a one-stop test management platform developed by HUAWEI CLOUD, meets customers' requirements for system security tests and acceptance tests.

CodeArts supports cloud development and provides visualized and customizable automatic delivery pipelines to help achieve continuous cloud delivery. CodeArts covers the entire lifecycle of software delivery, provides end-to-end software R&D support, and fully supports customers in implementing DevOps. CodeArts adds multiple security protection functions to ensure the security of core assets. Customers can embed their security lifecycle into the software development production line to form an automated DevSecOps security lifecycle management process, ensuring that information security is designed and implemented in the development lifecycle.

- **API Gateway**

API Gateway (APIG) is a high-performance, high-availability, and high-security API hosting service provided by HUAWEI CLOUD. It helps customers in two aspects. As an API provider, customers can use mature service capabilities (such as services and data) as backend services. Open APIs on APIG and provide them for API callers offline or release them to the API market to monetize service capabilities. As an API caller, customers can obtain and invoke APIs provided on APIG, reducing development time and costs. APIG supports API lifecycle management, version management, environment variable creation, traffic control and

monitoring. It also provides security protection components, such as access control and signature keys, to help customers control IP addresses and accounts for accessing APIs and ensure the security of backend services requested by APIG. Prevents unauthorized disclosure and modification of information in the service.

- **CodeArts PerfTest**

CodeArts PerfTest (formerly CPTS) is a cloud service that provides API and E2E performance tests of applications, which are built based on HTTP, HTTPS, TCP, or UDP. The rich capability of test model definition can be used to restore scenarios of large-scale concurrent service access, helping users identify application performance problems in advance.

- **CodeArts Check**

CodeArts Check is a self-developed code check service. Based on Huawei's 30-year experience in automatic source code static check technology and enterprise-level application, Huawei provides users with rich check capabilities, such as code style, general quality, and cyber security risks. It provides comprehensive quality reports and convenient closed-loop problem handling to help enterprises effectively control code quality and facilitate enterprise success.

7 Conclusion

HUAWEI CLOUD always adheres to HUAWEI's “customer-centric” core values and commit to protect customers data security resulting in the establishment of an information security management system and the deployment of the most common data security protection technologies in the industry to ensure 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 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' cardholder data environment when using HUAWEI CLOUD. Customers should evaluate their own operation and certification requirements, selecting appropriate cloud products and services, and properly configuring them.

8 Version History

Date	Version	Description
2024-08	2.2	Routine Update
2023-12	2.1	Routine Update
2023-10	2.0	Updated according to the new ISO 27001 standard
2022-03	1.1	Routine Update
2021-07	1.0	First Publication

