HUAWEI CLOUD Compliance with ISO/IEC 27001

Issue 1.0

Date 2021-07-16

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

1.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and 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 27001:2013, 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 27001:2013, developed the overall information security policy of HUAWEI CLOUD, and obtained the ISO/IEC 27001:2013 certification.

This document describes HUAWEI CLOUD's overall information security policies and specific control measures by responding to the requirements of ISO/IEC 27001:2013 and the 14 control domains in Appendix A, helping customers understand:

- Main control requirements of ISO/IEC 27001:2013 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 27001:2013.

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 165 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.

2 ISO 27001 Introduction

2.1 Framework and Main Contents of ISO 27001

ISO/IEC 27001:2013 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.

ISO/IEC 27001:2013 Information technology - Security techniques - 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.

Controls are summarized into 14 control domains, when an organization properly implements security controls, they can help organizations achieve and maintain information security compliance by addressing specific issues identified in formal periodic risk assessments.

The 14 security domains in ISO/IEC 27001:2013 and their brief introduction as follows:

- A.5 Information security policies: Provide management guidance and support for information security based on business requirements and relevant laws and regulation.
- A.6 Organization of information security: Establish a management framework to carry out the information security work of the organization.
- A.7 Human resource security: ensure that employees and outsourcing parties understand and fulfill their information security responsibilities and protect the company’s interests in the event of termination of employment.
- A.8 Asset management: Identify the organization’s information assets and determine the appropriate protection level based on the importance of the

information assets. Ensure that information assets stored in the media are not compromised or destroyed.

- A.9 Access control: Restricts access to information and information processing facilities, guarantees authorized users' access to systems and services, and prevents unauthorized access.
- A.10 Cryptography: Effective use of cryptographic techniques to protect the confidentiality, authenticity and integrity of information.
- A.11 Physical and environmental security: Prevent unauthorized physical access, damage and interference to information and information processing facilities. Prevent assets from being lost, damaged, stolen, or endangering the security of assets and business continuity.
- A.12 Operations security: Ensure correct and secure operation of information processing facilities and adopt technical means to prevent malicious code. Use backups to prevent data loss, use logging and monitoring to record situations and generate evidence. Ensure the integrity of the operating system, prevent the exploitation of technical vulnerabilities, and minimize the impact of audit activities on system operation.
- A.13 Communications security: Information in the network and its supporting information processing facilities shall be protected. Ensure the security of information transmitted inside and outside the company.
- A.14 System acquisition, development and maintenance: Information security is an integral part of the information system life cycle, and information security should be designed and implemented accordingly in the information system development life cycle. Data used for testing shall be protected.
- A.15 Supplier relationships: Ensure that information assets accessible to suppliers are protected. Maintain information security service delivery consistent with supplier agreements.
- A.16 Information security incident management: Manage information security incidents in an effective way, including communicating about security events and risks.
- A.17 Information security aspects of business continuity management: Integrate information security continuity into business continuity management. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
- A.18 Compliance: Avoid breach of laws, regulations, contractual obligations and any security requirements relating to information security. Conduct information security review and ensure that information security work is carried out in accordance with organizational policies and procedures.

2.2 Applicable Organization of Standard

The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

3 The Certification Status of HUAWEI CLOUD

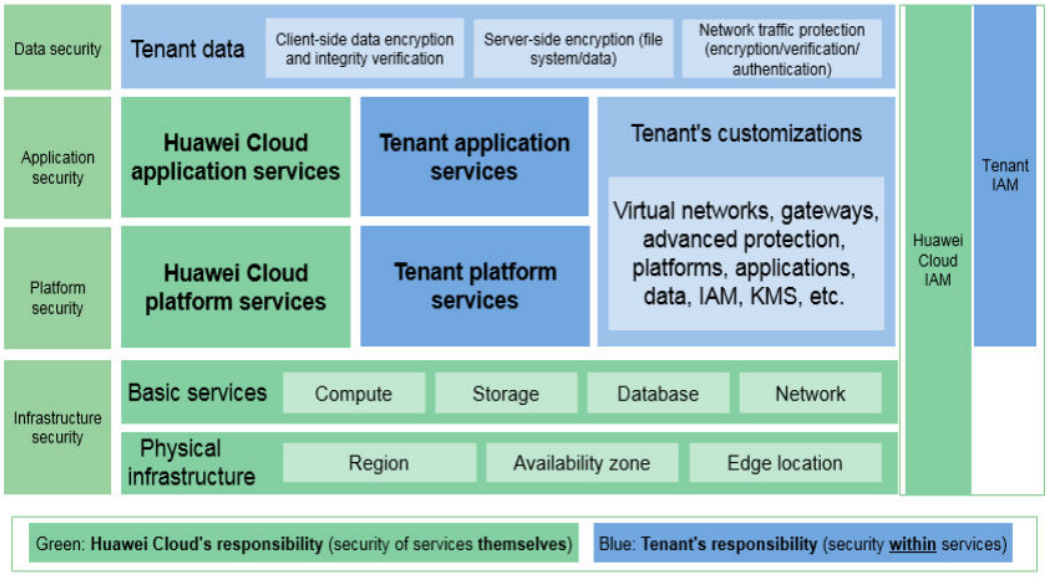
With its own information security system and security control management, HUAWEI CLOUD has obtained the ISO/IEC 27001:2013 certification. The certification covers products and services released by HUAWEI CLOUD on its official website, as well as data centers around the world.

For details about the certification scope and activity of ISO/IEC 27001:2013, 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 customer and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help customers 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 customer and HUAWEI CLOUD:

Figure 4-1 Responsibility Sharing Model



As shown in the above model, the privacy protection responsibilities are distributed between HUAWEI CLOUD and customers 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.

Customer: The primary responsibilities of the customers are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a customer 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 customer deploys on HUAWEI CLOUD. At the same time, the customer 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

The controls in the standard used in this document refer to GB/T 22080-2016/ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements published in 2016.

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 control objectives and controls

- **A.5 Information security policies**

  The objective of this control domain is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	HUAWEI CLOUD has implemented documented information security policies and procedures to provide guidance for HUAWEI CLOUD's operations and information security management. Information security policies and procedures must be approved by managers before released. Employees can access the released information security policies and procedures as authorized.
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	HUAWEI CLOUD reviews its information security management policy and procedures at least once a year and update as needed to reflect changes in the business objectives or risk environment. Changes in policies and procedures will be reviewed and approved by management.

- **A.6 Organization of information security**

  The objectives of this control domain are to establish a management framework to initiate and control the implementation and operation of information security within the organization, and to ensure the security of teleworking and use of mobile devices.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	For each products and services' business units, the information security responsibilities of all employees corresponding to their roles are clearly defined. HUAWEI CLOUD assigns roles dedicated to security and privacy protection to take certain information security management responsibilities. Information security-related roles and responsibilities are identified in writing and approved by management.
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	HUAWEI CLOUD follows the principle of separation of duties and checks and balances of authority. Separates incompatible duties and realizes reasonable division of authority. In addition, HUAWEI CLOUD has developed SOD separation of authority and responsibility management matrix to help realize this management principle.
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	HUAWEI CLOUD is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies.
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Same as A.6.1.3

A. 6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	HUAWEI CLOUD integrates security objectives into project objectives in project management, evaluates information security risks at the early stage of the project, and periodically reviews information security impacts during the entire project delivery process.
A. 6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	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.

A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	HUAWEI CLOUD employees use unique identity in the working network. If the external network needs to be connected to HUAWEI's 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. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing. For remote management of HUAWEI CLOUD, whether from the Internet or Huawei corporate network, one must first connect to HUAWEI CLOUD's bastion server environment, and then access target resources from a bastion server.

- **A.7 Human resource security**

  The objectives of this control domain are to ensure prior to employment, employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, to ensure that employees and contractors are aware of and fulfil their information security responsibilities during employment, and to protect the organization's interests as part of the process of changing or terminating employment.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall 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.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their 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. For external personnel, HUAWEI CLOUD signs a non-disclosure agreement with them and conducts information security training, including information security responsibilities.

A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established 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.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	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.

A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	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.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	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.8 Asset management**

  The objectives of this control domain is are to identify organizational assets and define appropriate protection responsibilities, to ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

No.	Control Domain	Control	HUAWEI CLOUD's response
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	According to the ISO27001 standard, HUAWEI CLOUD's information asset classification is monitored and managed by special tools to form an asset list, and each asset is assigned an owner.
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Same as A.8.1.1

A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities 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.
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	HUAWEI CLOUD has formulated personnel security 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.

A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	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 specifies 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.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Same as A.8.2.1
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Same as A.8.2.1

A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	HUAWEI CLOUD has formulated and implemented regulations on mobile media management. All types of mobile media are managed by dedicated 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.
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	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.
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Same as A.8.3.1

- **A.9 Access control**

  The objectives of this control domain are to limit access to information and information processing facilities, to ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information, and to prevent unauthorized access to systems and applications.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed 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.
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	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.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	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.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Same as A.9.2.1

A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	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. 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. Employees must use multi-factor authentication to determine their identities each time they log in.
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	HUAWEI CLOUD has formulated password policies and account security management regulations to 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.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	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. For a dedicated account, the account/right owner reviews the dedicated account he/she is responsible for, changes the password when the dedicated account is no longer needed, and notifies the new user. 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.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Same as A.9.2.5
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Same as A.9.2.4
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	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.

A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	HUAWEI CLOUD emphasizes that the security risks of employee cloud service accounts are controllable, strong security passwords are strictly required, account permissions are regularly reviewed, and privileged accounts are strictly managed and recycled. **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. **IAM** also provides session timeout policies, account login policies, and account locking policies.
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	HUAWEI CLOUD has formulated and implemented password policies, 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.

A.9.4.4	Use of privileged utility programs	The use of utility programs that might 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.
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	The HUAWEI CLOUD information security environment is managed by partitions. 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.10 Cryptography**

  The objective of this control domain is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

No.	Control Domain	Control	HUAWEI CLOUD's response

A. 10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	HUAWEI CLOUD has formulated and implemented cryptographic algorithm application specifications, which specify the selection and application rules of cryptographic algorithms, and provides guidance on common application instances.
A. 10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	HUAWEI CLOUD has formulated and implemented key management security specifications to manage security in each phase of the key lifecycle.

- **A.11 Physical and environmental security**

  The objectives of this control domain are to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities, and to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	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.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Same as A.11.1.1

A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Same as A.11.1.1
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	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.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Same as A.11.1.1

A. 11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	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. HUAWEI CLOUD uses physical and logical control to divide production and non-production environments. The data center reasonably divides the physical area of the computer room (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.

A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	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.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	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 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. 11.2.3	Cabling security	Power and telecommunications cabling carrying 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. 11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	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.
A. 11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	HUAWEI CLOUD has formulated regulations on managing storage media and devices in and out of data center, requiring that storage media and devices be registered and authorized before entering or leaving data center. Data leakage prevention management is implemented when physical storage media enters and exits data center, and data erasure and scrapping processes are specified to reduce possible data leakage losses.

A. 11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	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. 11.2.7	Secure disposal or reuse of equipment	All 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.
A. 11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	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. 11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	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.12 Operations security**

  The objectives of this control domain are to ensure correct and secure operations of information processing facilities, to ensure that information and information processing facilities are protected against malware, to protect against loss of data, to record events and generate evidence, to ensure the integrity of operational systems, to prevent exploitation of technical vulnerabilities, and to minimize the impact of audit activities on operational systems.

No.	Control Domain	Control	HUAWEI CLOUD's response
A. 12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	HUAWEI CLOUD implements documented information security policies and procedures to provide guidance for HUAWEI CLOUD's operations related to information processing and communications facilities. Employees can view the released information security policies and procedures under authorization.

A. 12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	HUAWEI CLOUD has established the system change management and service launch process, and communicated its requirements to all relevant developers (including internal employees and external partners). The newly launched or changed services shall follow the regulations of HUAWEI CLOUD release and change management process. 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.
A. 12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	HUAWEI CLOUD has established a complete resource management mechanism to plan the capacity of the resources in HUAWEI's unified virtualization platform to avoid excessive use of resources and meet capacity requirements. In addition, HUAWEI CLOUD collects component capacity information of cloud services to monitor the stable operation of the platform.

A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	HUAWEI CLOUD uses a combination of physical and logical control isolation methods for production and non-production environments, and controls the combined isolation methods to improve the network's partition self-protection and fault-tolerant recovery capabilities in the face of intrusions and internal ghosts, reducing risks of unauthorized access or changes to the running environment.

A. 12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	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 continuously educates employees on security awareness during their employment. A dedicated information security awareness training program is provided, including malware prevention.

A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	User data can be replicated and stored on multiple nodes in a data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery. Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, HUAWEI CLOUD also has a formal business continuity plan (BCP) and conducts BCP drills periodically.

A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	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.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Same as A.12.4.1
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Same as A.12.4.1

A.12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	HUAWEI CLOUD uses a standard protocol to synchronize time in the system.
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software 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.

A. 12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	HUAWEI CLOUD has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures. HUAWEI CLOUD announces the vulnerabilities of products or services that have been discovered on its official website and fore warns customers. Customers can check the **Security Notice** to be aware of the scope of the vulnerabilities, how to deal with them, and the threat level.
A. 12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	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.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	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.

- **A.13 Communications security**

  The objectives of this control domain are to ensure the protection of information in networks and its supporting information processing facilities, and to maintain the security of information transferred within an organization and with any external entity.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.13.1.1	Network controls	Networks shall be 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. 13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	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. 13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on 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. For further information about security zones, please refer to the **HUAWEI CLOUD Security White Paper**.

A. 13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	HUAWEI CLOUD has formulated security management regulations, defined information transmission policies and processes, and detailed control requirements.

A. 13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	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: HUAWEIcomplianc 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.
A. 13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	HUAWEI CLOUD protects information sent in electronic messages by using office computer security software, network access control, permission management, access control, transmission encryption, and content encryption.

A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	HUAWEI CLOUD regulates information confidentiality and non-disclosure agreement signing and archiving, and regularly updates the non-disclosure agreement templates that employees and external parties must sign.

- **A.14 System acquisition, development and maintenance**

  The objective of this control domain is to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. The objective of development and support processes is to ensure that information security is designed and implemented within the development lifecycle of information systems, and to ensure the protection of data used for testing.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	HUAWEI CLOUD manages the end-to-end software and hardware lifecycle through complete systems and processes, as well as automated platforms and tools. The lifecycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified, the design engineer will formulate mitigation measures according to the reduction library and the security design library and complete the corresponding security design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the security of products and services.

A. 14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	HUAWEI CLOUD uses multiple security measures to protect data involved in application services provided on public networks. **IAM**is used for access control and user identity authentication. Secure encryption channels (such as HTTPS) are used during information transmission, and stored static data is encrypted using secure encryption algorithms to ensure data confidentiality in different states. Control mechanisms such as digital signatures and timestamps are used to prevent tampering during data transmission, ensure information integrity, and prevent replay attacks. Logs are recorded for operations in application services to support audit. Identity authentication, transmission protection, and border protection for interfaces are performed to ensure API application security.

A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Same as A.14.1.2
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	By leveraging HUAWEI's wealth of experience and far-reaching capabilities in the field of security, HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also 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.

A. 14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	HUAWEI CLOUD has established the system change management and service launch process, and communicated its requirements to all relevant developers (including internal employees and external partners). The newly launched or changed services shall follow the regulations of HUAWEI CLOUD release and change management process.
A. 14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	HUAWEI CLOUD has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of HUAWEI CLOUD Change Committee.
A. 14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Same as A.14.2.3

A. 14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	HUAWEI CLOUD has formulated the public cloud service quality requirements, including the security design specification set, which defines system security engineering principles and applies them to service design.
A. 14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	HUAWEI CLOUD has pursued the new DevOps process, which features rapid and continuous iteration capabilities, and integrated the HUAWEI security development lifecycle (SDL). In addition, gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD hierarchically manages the development environment and implements protection measures such as physical isolation, logical isolation, access control, and data transmission channel approval and audit.

A. 14.2.7	Outsourced development	The organization shall supervise and monitor the activity of 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.
A. 14.2.8	System security testing	Testing of security functionality shall be carried out during development.	All cloud services pass multiple security tests before release. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. For further information, please refer to the **HUAWEI CLOUD Security White Paper**. 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.
A. 14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Same as A.14.2.8
A. 14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	HUAWEI CLOUD has formulated specifications for selecting and protecting test data, which are strictly followed during test work.

- **A.15 Supplier relationships**

  The objectives of this control domain are to ensure protection of the organization’s assets that is accessible by suppliers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

No.	Control Domain	Control	HUAWEI CLOUD's response
A. 15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets shall be agreed with the supplier and documented.	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. 15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information.	Supplier security and privacy requirements are included in signed contractual agreements. Business associates with third parties are responsible for managing their third-party relationships, including asset protection requirements and suppliers’ access to relevant applications. The HUAWEI CLOUD legal team also regularly reviews contract clauses.

A. 15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product 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.
A. 15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Same as A.15.1.1
A. 15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	HUAWEI CLOUD has formulated general procurement change management regulations and processes to strictly manage supplier service changes according to the management regulations. 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.

- **A.16 Information security incident management**

  The objective of this control domain is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	HUAWEI CLOUD has developed a mechanism for internal security incident management, includes commonly used security incident response plans and processes, and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. 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, continuous monitoring and real-time analysis ensure the timely detection of security incidents. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate.

A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	HUAWEI CLOUD has formulated the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation.

A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	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.
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	HUAWEI CLOUD has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Same as A.16.1.1

A. 16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	HUAWEI CLOUD uses a professional security incident management system to record and track the progress, handling measures, and implementation of all information security incidents, analyze the impact of incident handling, and track and close security incidents in an end-to-end manner to ensure that the entire handling process can be traced.
A. 16.1.7	证据的收集	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	HUAWEI CLOUD has developed security incident emergency handling process and response process. When a server or application is suspected to be intruded, security responders collect evidence for analysis.

- **A.17 Information security aspects of business continuity management**

  The objectives of this control domain are that information security continuity shall be embedded in the organization’s business continuity management systems, and the availability of information processing facilities should be ensured.

No.	Control Domain	Control	HUAWEI CLOUD's response

A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	HUAWEI CLOUD has obtained the certification of the ISO22301 business continuity management system standard, established a business continuity management system internally, and formulated a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies.
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Same as A.17.1.1
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	The HUAWEI CLOUD security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan. When significant changes take place in the organization and environment of HUAWEI CLOUD, the effectiveness of business continuity level would also be tested.

A. 17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	HUAWEI CLOUD deploys the multi-region and multi-AZ architecture adopted by the data center cluster to implement redundant connection of multiple AZs, eliminating the risk of single points of failure and ensuring service continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center to implement N+1 deployment in data centers. If a data center is faulty, traffic can be balanced to other data centers.

- **A.18 Compliance**

  The objectives of this control domain are to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements, and to ensure that information security is implemented and operated in accordance with the organizational policies and procedures through information security reviews.

No.	Control Domain	Control	HUAWEI CLOUD's response
A. 18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	HUAWEI CLOUD has established a dedicated position to maintain active contact with external parties, and to track the change of 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 ensure compliance with laws and regulations.

A. 18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	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. At the contract level, HUAWEI CLOUD fulfills the contract strictly according to the agreement with the supplier.
A. 18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	HUAWEI CLOUD has formulated data security policies and data security protection management regulations. Appropriate protection measures are taken and strictly implemented to ensure data security.
A. 18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	HUAWEI CLOUD has built 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.
A. 18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	HUAWEI CLOUD uses strong encryption algorithms widely accepted in the industry to encrypt data on the platform and uses encryption protocols to ensure data security during transmission.

A. 18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	HUAWEI CLOUD has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators. In addition, independent third-party assessment agencies also provide independent assurance. These auditors assess the security, integrity, and confidentiality of information and resources by performing regular security assessments and compliance audits or inspections (such as SOC, ISO standards, PCIDSS audits), so as to conduct independent assessment of risk management content/ process.
A. 18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Same as A.18.2.1

A. 18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. For all security vulnerability information known, HUAWEI CLOUD will evaluate and analyze each vulnerability, formulate and implement vulnerability fix plans or circumvention measures, and verify the fix situation after fixed, and continue tracking to confirm that the risk is eliminated or mitigated. HUAWEI CLOUD organizes internally or external third parties with certain qualifications to conduct penetration tests on all HUAWEI CLOUD systems and applications every six months, and follow up and rectify the results of penetration tests. The penetration test report and follow-up would be verified by internal audits and external certification agencies.

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 control domain.

ISO 27001 Control Domain	Products that Help in Achieving the Objectives
A.8 Asset management	**Data Security Center (DSC)**, **Host Security Service (HSS)**, **Object Storage Service (OBS)**
A.9 Access control	**Identity and Access Management (IAM)**
A.10 Cryptography	**Data Encryption Workshop (DEW)**

A.12 Operations security	**Vulnerability Scan Service (VSS)**, **Web Application Firewall (WAF)**, **Host Security Service (HSS)**, **Cloud Eye Service (CES)**, **Log Tank Service (LTS)**, **Database Security Service (DBSS)**, **Cloud Trace Service (CTS)**, **Cloud Backup and Recovery (CBR)**, **Elastic Volume Service (EVS)**, **Image Management Service (IMS)**, **Object Storage Service (OBS)**, **Dedicated Distributed Storage Service (DSS)**, **Scalable File Service (SFS)**, **Simple Message Notification (SMN)**
A.13 Communications security	**Virtual Private Cloud (VPC)**, **Virtual Private Network (VPN)**, **Anti-DDoS**, **Advanced Anti-DDoS (AAD)**, **SSL Certificate Manager (SCM)**, **Elastic Load Balance (ELB)**, **Direct Connect (DC)**, **Cloud Connect (CC)**
A.14 System acquisition, development and maintenance	**API Gateway (APIG)**, **Cloud Performance Test Service (CPTS)**,
A.15 Supplier relationships	**Cloud Eye Service (CES)**, **Application Operations Management (AOM)**
A.17 Information security aspects of business continuity management	**Cloud Backup and Recovery (CBR)**, **Cloud Server Backup Service (CSBS)**, **Storage Disaster Recovery Service (SDRS)**
A.18 Compliance	**Content Moderation**

6.1 A.8 Asset Management

When establishing an information security management system (ISMS), customers should identify the information assets they need to protect and define appropriate protection responsibilities to ensure that information is protected at an appropriate level according to its importance, and to prevent unauthorized disclosure, modification, removal or destruction of information stored in the media.

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.

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 .

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.

6.2 A.9 Access Control

Restricting access to information and information processing facilities, ensuring that authorized users have access to the systems and services they need, while preventing unauthorized access, are important objectives for customers to implement access control.

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.

6.3 A.10 Cryptography

Customers shall ensure that cryptographic technology is used appropriately and effectively to protect the confidentiality, authenticity and integrity of information.

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.

6.4 A.12 Operations Security

Customers' objectives of operation security include ensuring secure operation of information processing facilities, preventing malicious software, using backups to prevent data loss, using logging and monitoring to record situations and generate evidence, implementing software control to ensure the integrity of the operating system, preventing the use of technical vulnerabilities and consider minimizing the impact of operating system audit activities. HUAWEI CLOUD provides customers with a variety of cloud services to assist in achieving these operation security objectives.

Customers can use HUAWEI CLOUD to provide **Vulnerability Scan Service (VSS)**, scan web applications, operating systems, and configuration baselines, and check asset content compliance and weak passwords to identify security risks of websites or servers exposed to the network. HUAWEI CLOUD will immediately analyze and update rules for common CVE vulnerabilities and provide quick and professional CVE vulnerability scanning. 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. 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.

Cloud Eye Service (CES) provided by HUAWEI CLOUD helps customers monitor server running status and cloud resource usage in real time. When a hardware fault occurs, CES notifies customers by email, SMS, or HTTP/S. **Log Tank Service (LTS)** on HUAWEI CLOUD collects, queries, and stores logs in real time. It 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 (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.

If customers need to back up service data, software, and system images, HUAWEI CLOUD provides multiple products and services with different priorities. 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. 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.

6.5 A.13 Communications Security

Customers' communications security objectives include protecting information and information processing facilities in the network. Maintaining the security of information transmitted within the organization and between the organization and external entities.

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.

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.

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** provides 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 **Advanced Anti-DDoS (AAD)** service of HUAWEI CLOUD to detect and clean large-traffic attacks.

SSL Certificate Manager (SCM) of HUAWEI CLOUD provides customers with one-stop certificate lifecycle management, implementing trusted identity authentication and secure data transmission for websites. 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.

6.6 A.14 System Acquisition, Development and Maintenance

Customers should integrate information security into the information system lifecycle to ensure that information security is designed and implemented in the information system development life cycle.

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.

6.7 A.15 Supplier Relationships

In the control domain of supplier relationships, the main information security objective of customers is to ensure the information security level and service delivery quality of suppliers.

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 (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.

6.8 A.17 Information Security Aspects of Business Continuity Management

Customers shall integrate information security continuity into the organization's business continuity management and shall ensure the availability of information processing facilities.

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.

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.

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.

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 References

GB/T 22080-2016/ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

9 Version History

Date	Version	Description
2021-7	1.0	First Publication

