HUAWEI CLOUD Practical Guide for NIST CSF

Issue	1.0
Date	2022-05-23

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Scope of Application

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

1.2 Purpose of Publication and Target Audience

The NIST CSF is developed by the National Institute of Standards and Technology (NIST). The Cybersecurity Framework (CSF) was developed to provide guidance for organizations seeking to strengthen their cybersecurity defenses and better manage cybersecurity risks. Currently, this Framework has become a globally recognized security evaluation system. After being evaluated by an independent third-party organization, HUAWEI CLOUD has obtained the NIST CSF certification.

This document describes how HUAWEI CLOUD builds or improves cybersecurity and risk management capabilities based on the NIST CSF, helping customers understand:

- How HUAWEI CLOUD builds a Cybersecurity System based on NIST CSF;
- HUAWEI CLOUD offers multiple products and services to customers to help them implement the NIST CSF.

2 NIST CSF Introduction

2.1 Basic Definition

- **HUAWEI CLOUD**

HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.

- **Customer**

Refers to a registered user in a business relationship with HUAWEI CLOUD.

- **Critical Infrastructure**

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.

- **Mobile Code**

A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

- **Framework Core**

A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

- **Framework Implementation Tier**

A lens through which to view the characteristics of an organization’s approach to risk-how an organization views cybersecurity risk and the processes in place to manage that risk.

- **Framework Profile**

A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

2.2 Evolution of NIST CSF

To enhance the resilience of U.S. critical infrastructure to address cybersecurity risks, the Cybersecurity Enhancement Act of 2014 (CEA) updated the role of NIST, to include developing a cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. This formalized NIST's previous work developing Framework Version 1.0 under Executive Order 13636 "Improving Critical Infrastructure Cybersecurity (February 2013)", and provided guidance for future Framework evolution. The Framework that developed under EO 13636 and continues to evolve according to CEA, uses common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

In April 2018, NIST refines, clarifies, and enhances Version 1.0 and released NIST CSF Version 1.1, incorporating comments received on the drafts of Version 1.1.

2.3 Applicable groups of the Framework

NIST CSF is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT).

2.4 NIST CSF and Key Contents

NIST CSF consists of three parts: the Framework Core, the Implementation Tiers and the Framework Profiles. The Framework Core consists of five concurrent and continuous Functions—Identify Protect Detect Respond Recover. This capability Framework covers the entire cybersecurity process before, during, and after the event, helping enterprises proactively identify, prevent, detect, and respond to security risks.

The five functional elements of the Framework are described as follows:

- Identify - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- Protect - Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- Detect - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- Respond - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- Recover - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

3 The Certification Status of HUAWEI CLOUD

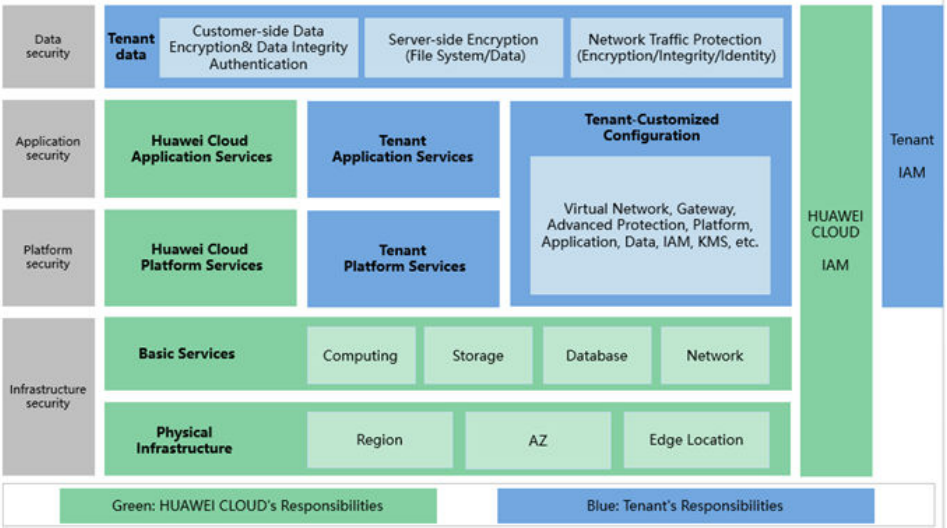
HUAWEI CLOUD has obtained the highest NIST CSF Tier4 certification issued by the British Standards Institution (BSI), which is the first cloud service provider in China to obtain the NIST CSF certification. It indicates the maturity of HUAWEI CLOUD's capabilities in risk detection, handling, response, and recovery, and indicates that HUAWEI CLOUD has the capability to provide secure and reliable cloud services for global users.

The certification covers products and services released on HUAWEI CLOUD's official website and data centers around the world. For details about NIST CSF certification, visit HUAWEI CLOUD **Trust Center** to apply for downloading the NIST CSF evaluation report.

4 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 4-1 Responsibility Sharing Model


Data security
Tenant data
Customer-side Data Encryption& Data Integrity Authentication
Server-side Encryption (File System/Data)
Network Traffic Protection (Encryption/Integrity/Identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Tenant-Customized Configuration
Virtual Network, Gateway, Advanced Protection, Platform, Application, Data, IAM, KMS, etc.
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
Basic Services
Computing
Storage
Database
Network
Physical Infrastructure
Region
AZ
Edge Location
HUAWEI CLOUD IAM
Tenant IAM
Green: HUAWEI CLOUD's Responsibilities
Blue: Tenant's Responsibilities

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

HUAWEI CLOUD: The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross-layer function.

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

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

5 How HUAWEI CLOUD Builds a Cybersecurity System Based on the NIST CSF

HUAWEI CLOUD optimizes the cybersecurity system based on the NIST CSF, and maintains and continuously improves the system based on the PDCA cycle model during daily operations. However, this does not mean that customers can pass the NIST CSF certification if they use HUAWEI CLOUD services. The customer and HUAWEI CLOUD share security responsibilities based on the preceding responsibility matrix. The customer should take corresponding measures based on their own situation.

5.1 Identify

Category	Subcategory	Informative References	Measures Taken by HUAWEI CLOUD	Recommended Actions for Customer
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes	ID.AM-1: Physical devices and systems within the organization are inventoried	ISO/IEC 27001:2013 A.8.1.1 A.8.1.2	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.	The customer is responsible for identifying and recording physical assets outside HUAWEI CLOUD. (e.g., servers, computers, network devices, mobile devices, IoT devices, peripherals, etc.) The customer is responsible for identifying and documenting the software

are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-2: Software platforms and applications within the organization are inventoried	ISO/IEC 27001:2013 A.8.1.1 A.8.1.2 A.12.5.1	Same as ID.AM-1	platform and application list and ensuring that the information recorded accurately reflects the current situation.
	ID.AM-3: Organizational communication and data flows are mapped	ISO/IEC 27001:2013 A.13.2.1 A.13.2.2	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 tolerance in HUAWEI CLOUD in response to attacks from external threat actors and internal threats. HUAWEI CLOUD will maintain the latest network topology. 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 through virtual private networks (VPNs).	The customer is responsible for controlling the flow of communication and data within the customer applications, and between the customer applications and external systems. The customer is responsible for authorizing connections to external and internal information systems as well as documenting the connection information.

	ID.AM-4: External information systems are catalogued	ISO/IEC 27001:2013 A.11.2.6	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. 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. In principle, free or open-source software downloaded from the network is not used. If the software needs to be installed due to service requirements, the software will be scanned by antivirus software.	The Customer is responsible for identifying and recording all external information systems.

	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	ISO/IEC 27001:2013 A.8.2.1	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.	The customer is responsible for prioritizing resources based on their classification, criticality, and business value, and defining its priority based on the criteria listed.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ISO/IEC 27001:2013 A.6.1.1	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.	The customer is responsible for identifying the cybersecurity roles and responsibilities of the company and its third-party stakeholders, for establishing security requirements for third-party stakeholders, and for monitoring compliance with third-party service providers

Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization’s role in the supply chain is identified and communicated	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2	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. 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. 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.	The customer is responsible for identifying, documenting and communicating their role in the supply chain.

	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	ISO/IEC 27001:2013 Clause 4.1	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	The customer is responsible for identifying, documenting, and communicating roles in critical infrastructure.

			administrative agencies, risk and compliance organizations, local authorities and regulatory agencies and establish contact points.	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	N/A	Same as ID.BE-2	The customer is responsible for identifying, documenting, and communicating priorities for their organizational mission and business objectives.

	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2 A.11.2.3 A.12.1.3	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. 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	The customer is responsible for identifying, documenting and communicating dependencies for critical service delivery.

			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. 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.	

	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/ attack, during recovery, normal operations)	ISO/IEC 27001:2013 A.11.1.4 A.17.1.1 A.17.1.2 A.17.2.1	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. For risks such as intrusion and authorization a monitoring and response mechanism has been established as well. 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. HUAWEI CLOUD has obtained the certification of the ISO22301 business	The customer is responsible for identifying the resiliency requirements of the system and selecting the region and AZ where the service is located.

			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.	
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational cybersecurity policy is established and communicated	ISO/IEC 27001:2013 A.5.1.1	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.	The customer is responsible for developing their organization's information security policies and procedures to inform cybersecurity risk management.

	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	ISO/IEC 27001:2013 A.6.1.1 A.7.2.1 A.15.1.1	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. 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	The customer is responsible for identifying and documenting information security roles and responsibilities and developing and implementing a cybersecurity plan, including roles and responsibilities of internal and external stakeholders, as well as communication and coordination methods.

			well as punishment measures for information security violations in the contract or agreement signed with them. 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.	

	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ISO/IEC 27001:2013 A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5	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. 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.	The customer is responsible for identifying cybersecurity-related laws and regulations and for developing, documenting and disseminating policies regarding these compliance requirements.

	ID.GV-4: Governance and risk management processes address cybersecurity risks	ISO/IEC 27001:2013 Clause 6	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.	The customer is responsible for developing, documenting and disseminating cybersecurity risk management policies.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	ISO/IEC 27001:2013 A.12.6.1 A.18.2.3	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. HUAWEI CLOUD has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial	The customer is responsible for developing a vulnerability management mechanism, following the vulnerability scanning process, scanning its information systems (e.g., customer applications, databases, and operating systems) for vulnerabilities at a frequency defined by the organization, recording and analyzing the vulnerability scanning results, and completing vulnerability remediation within the defined response time.

			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.	

	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	ISO/IEC 27001:2013 A.6.1.4	Huawei PSIRT has established a comprehensive vulnerability awareness and collection channel. The vulnerability collection email address psirt@huawei.com and the vulnerability reward program https://bugbounty.huawei.com/hbp have been published on PSIRT, which encourages global vulnerability coordination organizations, suppliers, security companies, organizations, security researchers, and Huawei employees to submit vulnerabilities in Huawei products or solutions. In addition, Huawei PSIRT proactively monitors the industry's well-known vulnerability database, security forums, mailing lists, and security conferences to ensure that Huawei-related vulnerability information, including the cloud, is immediately detected. Establish a corporate-level vulnerability database for all products and solutions, including cloud services, to ensure that each vulnerability is effectively recorded, tracked, and closed. In addition, HUAWEI	The customer is responsible for collecting and analyzing cyber threat intelligence from the information sharing platform, generating internal security alerts as necessary, and disseminating them to relevant personnel.

			CLOUD has set up a dedicated vulnerability collection email address hws_security@huawei.com. The security O&M team of HUAWEI CLOUD uses self-developed and commercial online security scanning tools to regularly scan vulnerabilities (excluding tenant instances). Vulnerabilities in the HUAWEI CLOUD environment can be hidden and visualized.	
	ID.RA-3: Threats, both internal and external, are identified and documented	ISO/ IEC27001: 2013 Clause 6.1.2	Same as ID.GV-4	The customer is responsible for developing, documenting, and disseminating cybersecurity risk management policies, both internal and external.

	ID.RA-4: Potential business impacts and likelihoods are identified	ISO/ IEC27001: 2013 A.16.1.6 Clause 6.1.2	HUAWEI CLOUD is committed to customer data security and privacy protection. Based on international standards, HUAWEI CLOUD has established the Information Security Management System (ISMS) and Privacy Information Management System (PIMS). It has systematically conducted information security risk assessment and privacy impact assessment (PIA) to fully identify and analyze security and privacy risks. Formulate and implement measures to respond. Legal compliance and global compliance are important foundations for Huawei's survival, service, and contribution in the world. HUAWEI CLOUD is committed to strictly complying with all applicable laws and regulations in the countries where it is located, and systematically identifying and managing compliance risks from external regulations to internalizing and developing compliance redlines. In addition, the emergency response plan is established, and related training	The customer is responsible for assessing and documenting the likelihood of potential risks occurring and the impact on the business.

			and drills are conducted to improve the organization's compliance awareness and capability of responding to emergencies. In addition, HUAWEI CLOUD has established end-to-end business continuous improvement and optimization management from suppliers to HUAWEI CLOUD and from HUAWEI CLOUD to customers. By establishing policies, organizations, regulations, processes, baselines, and IT platforms, HUAWEI CLOUD conducts business impact analysis and risk assessment. Improve the organization's compliance with corporate regulations and process requirements, ensure effective management of daily business risks, ensure business continuity between HUAWEI CLOUD organizations and cloud services, and effectively support the stable operation and business operation of the customer's system.	

	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ISO/IEC 27001:2013 A.12.6.1	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 customer is responsible for developing risk assessment methods and assessing risks based on threats, vulnerabilities, risk occurrence probability, and risk impact.

	ID.RA-6: Risk responses are identified and prioritized	ISO/IEC 27001:2013 Clause 6.1.3	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.	The customer is responsible for analyzing the identified risks and prioritizing the risks based on the organization's defined risk tolerance.

Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	ISO/IEC 27001:2013 Clause 6.1.3 Clause 8.3 Clause 9.3	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. HUWEI CLOUD regularly conducts management reviews every year, identifies problems in the system operation, and implements rectifications to promote continuous	The customer is responsible for developing risk management strategies related to the information system. This strategy requires agreement from organizational stakeholders.

			improvement of the management system.	
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	ISO/IEC 27001:2013 Clause 6.1.3 Clause 8.3	Based on the risk, governance, and control framework, HUAWEI CLOUD conducts comprehensive and multi-dimensional risk management from data security, privacy protection, compliance, and operation to minimize risks of HUAWEI CLOUD services. In addition, the acceptable scope of risks is defined and the process and roles for decision-making on risk acceptance are defined.	The customer is responsible for determining the risk tolerance level of the organization and obtaining agreement from the organization's stakeholders.
	ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	ISO/IEC 27001:2013 Clause 6.1.3 Clause 8.3	In the risk identification phase, HUAWEI CLOUD analyzes business activities and takes the identified inherent risks and existing control measures as the decision-making factors for risk tolerance.	The customer is responsible for identifying different levels of risk tolerance based on industry standards and the importance of their systems.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2	Same as ID.BE-1	The customer is responsible for developing supply chain risk management processes that must be identified, established, accessed and managed by organizational stakeholders.
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	ISO/IEC 27001:2013 A.15.2.1 A.15.2.2	Same as ID.BE-1	The customer is responsible for accessing all partners and suppliers associated with critical information systems in accordance with the supply chain risk management process.

	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3	Same as ID.BE-1 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.	The customer is responsible for requiring their suppliers and partners to implement appropriate controls to achieve the objectives defined by the supply chain risk management process.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	ISO/IEC 27001:2013 A.15.2.1 A.15.2.2	Same as ID.BE-1	The customer is responsible for monitoring and reviewing their suppliers and partners to confirm that they have met their obligations as required.

	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	ISO/IEC 27001:2013 A.17.1.3	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.	The customer is responsible for developing the emergency response and recovery plan for its business system. If services provided by a third party are involved, the customer needs to perform tests with the third party.

5.2 Protect

Category	Subcategory	Informative References	HUAWEI CLOUD's Response	Customer's Responsibilities

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	ISO/IEC 27001:2013 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3	HUAWEI CLOUD employee account management complies with HUAWEI user account permission management regulations. For HUAWEI 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. 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. Identity and Access Management (IAM) is used to control and manage user access to cloud services. HUAWEI CLOUD has specified the maximum	The customer is responsible for developing, documenting, maintaining, disseminating, and implementing access control policies and support procedures. The customer is responsible for creating and managing user accounts using Identity and Access Management (IAM) of HUAWEI CLOUD.

			review period for accounts/ rights at different levels. The account/right owner periodically reviews the accounts/rights held by the account/right owner and submits a deregistration application when the user is transferred or the role changed. The management owner submits a deregistration application when the outsourced personnel leaves the site or no longer needs the account or permission. The supervisor will review whether the subordinate's account/ right is proper. If the subordinate's position/ role changes, the supervisor will review whether the subordinate's account/ right of the original position has been cancelled.	

	PR.AC-2: Physical access to assets is managed and protected	ISO/IEC 27001:2013 A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8	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 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. 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	N/A

			security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. 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. 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. 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. 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.	

	PR.AC-3: Remote access is managed	ISO/IEC 27001:2013 A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1	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. 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. 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	Customer is responsible for developing, documenting, maintaining, disseminating, and implementing access control policies and for developing usage specifications for the organization-controlled mobile devices based on their access control policies.

			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.	

	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	ISO/IEC 27001:2013 A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5	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. 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.	The customer is responsible for providing each user with the appropriate level of access, maintaining the appropriate segregation of duties and least privilege, based on the user's job function.

	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	ISO/IEC 27001:2013 A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3	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 multilayered security isolation, access control, and perimeter protection for physical and virtual networks. Based on business functions and network security risks, the HUAWEI CLOUD	The customer is responsible for managing network access for its applications hosted in HUAWEI CLOUD and using network segmentation, firewall, antivirus, and intrusion detection to protect network integrity.

			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 abovementioned 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.**	

	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	ISO/IEC 27001:2013 A.7.1.1 A.9.2.1	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. 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 onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off-boarding security review.	The customer is responsible for taking identification measures for the application to ensure the uniqueness of the identification, and the identification information is complex and periodically replaced. When the identification information of the user is lost or invalid, technical measures are taken to ensure the security of the identification information resetting process.

	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	ISO/IEC 27001:2013 A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4	Same as PR.AC-1 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. 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.	The customer is responsible for establishing protection measures for identity authentication, ensuring that the login failure processing function is available, configuring and enabling measures such as ending sessions, and limiting the number of illegal logins.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	ISO/IEC 27001:2013 A.7.2.2 A.12.2.1	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.	The customer is responsible for carrying out security awareness education and job skill training for internal personnel, and notifying them of relevant safety responsibilities and disciplinary measures. Develop different training and improvement plans for different positions.

	PR.AT-2: Privileged users understand their roles and responsibilities	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	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. HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers, including onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off-boarding security review. 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.	The customer is responsible for training users based on roles and responsibilities before they use privileged users and developing training plans for them.

	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	ISO/IEC 27001:2013 A.6.1.1 A.7.2.1 A.7.2.2	Same as PR.AT-2 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. 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. 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	The customer is responsible for establishing security roles and requirements of third-party stakeholders, reaching agreement with the third party on related content, forming formal documents, and specifying information security obligations of all parties in the service supply chain in the agreement signed with the selected service provider.

			asset protection requirements and suppliers' access to relevant applications. The HUAWEI CLOUD legal team also regularly reviews contract clauses.	
	PR.AT-4: Senior executives understand their roles and responsibilities	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	Same as PR.AT-2	The customer is responsible for training senior executives based on roles and responsibilities before they use privileged users and developing training plans accordingly.
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	Same as PR.AT-2	The customer is responsible for role- and responsibilities-based training of physical and cybersecurity personnel prior to using privileged users and for developing appropriate training plans.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	ISO/IEC 27001:2013 A.8.2.3	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. 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,	The customer is responsible for using cryptographic technologies to ensure the integrity and confidentiality of important data in storage. (for example, servers, PCs, or important components of the system)

			transmission protection, and border protection for interfaces are performed to ensure API application security.	
	PR.DS-2: Data-in-transit is protected	ISO/IEC 27001:2013 A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3	Same as PR.DS-1 HUAWEI CLOUD has formulated security management regulations, defined information transmission policies and processes, and detailed control requirements. 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.	The customer is responsible for protecting the data during transmission by adopting technical measures, including: using cryptography or verification technology to ensure the data integrity during communication, and using cryptography to ensure the confidentiality of important data or the entire message during communication.

	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	ISO/IEC 27001:2013 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7	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. 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. 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.	N/A

	PR.DS-4: Adequate capacity to ensure availability is maintained	ISO/IEC 27001:2013 A.12.1.3 A.17.2.1	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. 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.	Customers are responsible for monitoring and planning the capacity needs of their applications and tenant environments.

	PR.DS-5: Protections against data leaks are implemented	ISO/IEC 27001:2013 A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3	Same as PR.DS-1 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 onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off boarding security review. 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. HUAWEI CLOUD employees must sign the resignation confidentiality commitment letter to	The customer is responsible for adopting technical measures to protect data leakage, for example, developing data access control policies and encrypting important data.

			confirm their ongoing information security responsibilities. For external personnel, the contact departments sign non-disclosure agreements with their company based on service requirements. In terms of account and permission management, 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. HUAWEI CLOUD implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimized permission assignment and strict behavior audit ensure that unauthorized access is not performed. HUAWEI CLOUD 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 multifactor authentication to determine their identities each time they log in. In terms of physical access control, HUAWEI CLOUD divides the data center into multiple security areas based on business functions and network security risks, realizing physical and logical control. HUAWEI CLOUD O&M personnel must first log onto the Virtual Private Network (VPN) to connect to this security zone and then log onto managed nodes through bastion hosts. HUAWEI CLOUD administrator-level personnel can access O&M interfaces of all security zones from this security zone. This security zone does not expose its interfaces to any other security zone. The 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. In terms of storage media management, 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.	

	PR.DS-6: Integrity checking mechanisms are used to verify software, hardware, and information integrity	ISO/IEC 27001:2013 A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4	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 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	Customer is responsible for using integrity verification tools to monitor and detect unauthorized changes to software, hardware, and information.

			open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, software installation, and software exit. HUAWEI CLOUD 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. 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.	

	PR.DS-7: The development and testing environment(s) are separate from the production environment	ISO/IEC 27001:2013 A.12.1.4	HUAWEI CLOUD uses a combination of physical and logical control isolation methods for production and nonproduction 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. 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. HUAWEI CLOUD has formulated specifications for selecting and protecting test data, which are strictly followed during test work.	The customer is responsible for physically or logically isolating production and non-production environments and ensuring that test data and results are controlled.

	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	ISO/IEC 27001:2013 A.11.2.4	For data center maintenance, HUAWEI CLOUD has established regulations and processes related to data center O&M management, including specific device control measures and routine maintenance plans. HUAWEI CLOUD has formulated 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.	The customer is responsible for managing the lifecycle of applications running on its cloud, and provisions and monitors the health of the hardware under its control.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	ISO/IEC 27001:2013 A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	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. HUAWEI CLOUD ensures the secure introduction and use of open source and third-party software based on the principle of strict entry and wide use. HUAWEI CLOUD has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, software installation, and software exit. HUAWEI CLOUD has 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. HUAWEI CLOUD has formulated management regulations and change procedures for change management, before	The customer is responsible for formulating configuration management plans. During the entire lifecycle, the customer establishes and records configuration information about important information systems, products, and components, including the network topology, software components installed on each device, version and patch information of software components, and configuration parameters of each device or software component. Maintained in conjunction with the operating procedures and protected their confidentiality.

			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.	

	PR.IP-2: A System Development Life Cycle to manage systems is implemented	ISO/IEC 27001:2013 A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.5	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. 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	The customer is responsible for building a system development life cycle management mechanism and combining it with cybersecurity risk management to achieve synchronous planning, construction, and use of security technology measures.

			together ensure the smooth and flexible implementation of DevSecOps.	
	PR.IP-3: Configuration change control processes are in place	ISO/IEC 27001:2013 A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	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. HUAWEI CLOUD has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production like environment testing, pilot release, and/or blue/ green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of HUAWEI CLOUD Change Committee.	The customer is responsible for including the configuration information changes into the system change scope, controlling the configuration information changes, and updating the basic configuration information library in a timely manner. The customer is responsible for establishing change management procedures, controlling all changes according to the procedures, and recording the change implementation process. Monitor and evaluate the integrity of changes, record changes, analyze potential impacts, track the effect of defect rectification, and report to related personnel.

	PR.IP-4: Backups of information are conducted, maintained, and tested	ISO/IEC 27001:2013 A.12.3.1 A.17.1.2 A.17.1.3 A.18.1.3	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. 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.	The customer is responsible for disaster recovery and backup of critical systems and databases. The backup must meet the RTO and RPO objectives of the organization. Manages and maintains the backup data, and formulates the data backup policy, recovery policy, backup procedure, and recovery procedure according to the importance of the data and the impact of the data on the system running.

	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	ISO/IEC 27001:2013 A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3	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. 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. HUAWEI CLOUD strictly controls the electrical and fire safety. HUAWEI	N/A

			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. 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.	

	PR.IP-6: Data is destroyed according to policy	ISO/IEC 27001:2013 A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7	Same as PR.DS-1 HUAWEI CLOUD has formulated and implemented relevant media management regulations, in which the media are cleared and scrapped according to the classification. HUAWEI CLOUD achieves data cleaning, disk demagnetization through a variety of ways, and records the destruction operation. Dedicated personnel manage devices that contain storage media on HUAWEI CLOUD. After the devices are used, dedicated personnel format the devices. When a storage media that stores HUAWEI's confidential information is scrapped, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting.	N/A

	PR.IP-7: Protection processes are improved	ISO/IEC 27001:2013 A.16.1.6 Clause 9 Clause 10	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.	The customer is responsible for developing the corresponding control process for the safety protection measures taken by the organization, including: regularly verifying and reviewing the reasonableness and applicability of the safety objectives, safety management system, and safety plan, and revising the deficiencies or improvements that need to be made. Regularly conduct comprehensive security inspection, including the effectiveness of existing security technical measures, consistency between security configuration and security policy, and implementation of security management system.

	PR.IP-8: Effectiveness of protection technologies is shared	ISO/IEC 27001:2013 A.16.1.6	HUAWEI CLOUD is committed to building an open, collaborative, and win-win security ecosystem. Together with industry-leading security products and service providers, HUAWEI CLOUD provides cloud tenants with easy-to-deploy, easy-to-manage, and perfect security solutions based on the responsibility sharing mode to cope with known and unknown security threats. Ensures tenant data and service security. Facing security threats from the future intelligent society, HUAWEI CLOUD will work with global security partners to build an open, collaborative, and win-win security ecosystem. While continuously providing cloud security value-added services, improving user trust, we will spare no effort to promote industry and social progress.	The Client is responsible for sharing information within its purview with appropriate parties in a secure and acceptable environment. Customers can actively participate in the formulation of national and industry standards for cybersecurity, and provide cybersecurity-related education and training by educational and training institutions such as colleges and universities and vocational schools. They can train cybersecurity talents in various ways to promote the exchange of cybersecurity talents.

	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ISO/IEC 27001:2013 A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3	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. 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	The customer is responsible for developing incident response and business continuity plans, as well as incident and disaster recovery plans.

			security expert resources for response. 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.	
	PR.IP-10: Response and recovery plans are tested	ISO/IEC 27001:2013 A.17.1.3	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. HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate.	The customer is responsible for regular emergency plan training and drills for system-related personnel. The customer should develop drill scenarios based on possible risks and fully evaluate the response capability to different incidents.

	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	ISO/IEC 27001:2013 A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1 A.8.1.4	Before hiring an employee, 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 onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off boarding security review. 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. During personnel appointment, HUAWEI CLOUD has formulated information security management requirements for general	The customer is responsible for fully considering cybersecurity in HR management, including assigning or authorizing special departments or personnel to manage HR resources, establishing formal personnel security policies, and clearly defining objectives, scope, roles, responsibilities, management commitments, and organizational relationships.

			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. 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. 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. When an employee resigns, 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. 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.	

	PR.IP-12: A vulnerability management plan is developed and implemented	ISO/IEC 27001:2013 A.12.6.1 A.14.2.3 A.16.1.3 A.18.2.2 A.18.2.3	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 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. HUAWEI CLOUD announces the	The customer is responsible for taking necessary measures to identify security vulnerabilities and hidden dangers regularly and at important time nodes such as system launch and change, rectify the discovered security vulnerabilities and hidden dangers in time or assess the possible impact, and report to relevant departments. Security-related matters, such as security policies, malicious code, and patch upgrade, should be centrally managed. Regularly review the effectiveness of personnel, processes, and tools for risk assessment and vulnerability scanning and update them in a timely manner.

			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.	
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	ISO/IEC 27001:2013 A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6	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.	The customer is responsible for maintaining its own infrastructure, including the infrastructure connected to the HUAWEI CLOUD environment.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	ISO/IEC 27001:2013 A.11.2.4 A.15.1.1 A.15.2.1	Same as PR.AC-3	The customer is responsible for ensuring that non-local maintenance and diagnostic activities are approved and documented to prevent unauthorized access.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	ISO/IEC 27001:2013 A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	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.	The customer is responsible for formulating formal audit policies and documenting the purpose, scope, roles, responsibilities, and accountability system of log audit.
	PR.PT-2: Removable media is protected and its use restricted according to policy	ISO/IEC 27001:2013 A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.9	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.	N/A

	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	ISO/IEC 27001:2013 A.9.1.2	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. 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.	The customer is responsible for restricting unauthorized access to important information systems, products, and components according to the principle of functionality, and recording all unauthorized access attempts. All computing devices must comply with the minimal installation principle and install only required components and applications based on the whitelist technology.

	PR.PT-4: Communications and control networks are protected	ISO/IEC 27001:2013 A.13.1.1 A.13.2.1 A.14.1.3	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 abovementioned 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. HUAWEI CLOUD's efficient multi-dimensional full-stack protection system also	The customer is responsible for developing the network and communication mechanisms to protect the flow of information within the application and between the application and external systems. The customer is responsible for establishing and documenting usage restrictions, configuration and connectivity requirements, and implementation guidance for accessing the application.

			includes multiple border protection measures. HUAWEI CLOUD has adapted various advanced protection functions to the trust boundary between the intranet and extranet. For further information, please refer to the HUAWEI CLOUD Security White Paper.	
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	ISO/IEC 27001:2013 A.17.1.2 A.17.2.1	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. 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.	N/A

5.3 Detect

Category	Subcategory	Informative References	HUAWEI CLOUD's Response	Customer's Responsibilities

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	ISO/IEC 27001:2013 A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2	HUAWEI CLOUD refers to the CIS - Center of Internet Security - security baseline and incorporates it into the DevSecOps process of HUAWEI CLOUD services. All products must be checked by the security engineering lab according to the corresponding security configuration specifications before launch. Product configuration changes must comply with the change management process.	Data flow between components and information systems: The customer is responsible for ensuring that the data flow is authorized and approved according to the developed data flow control strategy. Control the data flow and update the data exchange protocol periodically according to the security protocol of the information system. In terms of network and system configuration management, the customer shall establish management system, make regulations on network and system configuration management, formulate configuration and operation manuals for important equipment, and perform safety configuration and optimization of

				equipment according to the manuals.

	DE.AE-2: Detected events are analyzed to understand attack targets and methods	ISO/IEC 27001:2013 A.12.4.1 A.16.1.1 A.16.1.4	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. 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	Based on the established monitoring policy, the customer enables audit records of information systems (such as networks, hosts, databases, and applications) and periodically checks and analyzes audit records to detect attacks. The customer should take technical measures to analyze network behavior. When an attack is detected, the customer records the attack source IP address, attack type, attack purpose, and attack time.

			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 has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents.	

	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	ISO/IEC 27001:2013 A.12.4.1 A.16.1.7	Same as DE.AE-2 HUAWEI CLOUD uses the situational awareness analysis system to correlate alarm logs of various security devices and perform unified analysis to quickly identify attacks that have occurred and predict threats that have not occurred.	The customer is responsible for correlating and analyzing security-related information gathered from multiple sources. Automated mechanisms are used to assist in tracking security incidents and gathering and analyzing incident information.
	DE.AE-4: Impact of events is determined	ISO/IEC 27001:2013 A.16.1.4	HUAWEI CLOUD has established a security incident response team to monitor and analyze alarms and assess whether they are information security 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.	When information systems and information processed, stored, or transmitted by the systems are accessed, used, disclosed, interrupted, modified, or damaged without authorization, the customer is responsible for analyzing the risks and impacts of such events.

	DE.AE-5: Incident alert thresholds are established	ISO/IEC 27001:2013 A.16.1.4	Same as DE.AE-2	The customer is responsible for classifying security incidents in advance and defining which security incidents need to be reported.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	DE.CM-1: The network is monitored to detect potential cybersecurity events	N/A	Same as DE.AE-2	The customer is responsible for formulating network monitoring policies, including determining monitoring indicators and monitoring frequency, and continuously monitoring cybersecurity according to the monitoring policies.

	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	ISO/IEC 27001:2013 A.11.1.1 A.11.1.2	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.	N/A

	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	ISO/IEC 27001:2013 A.12.4.1 A.12.4.3	Same as DE.AE-2	The customer is responsible for monitoring employee access to the environment for potential security incidents.

	DE.CM-4: Malicious code is detected	ISO/IEC 27001:2013 A.12.2.1	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	The customer is responsible for formulating malicious code prevention specifications, including authorized use of anti-malicious code software, malicious code library upgrade, and periodic malicious code check and kill. In addition, improve the anti-malicious code awareness of all users, and instruct external computers or storage devices to detect malicious code before accessing the system.

			on security awareness during their employment. A dedicated information security awareness training program is provided, including malware prevention.	
	DE.CM-5: Unauthorized mobile code is detected	ISO/IEC 27001:2013 A.12.5.1 A.12.6.2	Same as DE.CM-4	The customer is responsible for defining acceptable and unacceptable mobile code and mobile code technologies and establishing usage restrictions and implementation guidelines for acceptable mobile code and mobile code technologies.

	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	ISO/IEC 27001:2013 A.14.2.7 A.15.2.1	HUAWEI CLOUD has specified requirements on R&D outsourcing management, and incorporates the supervision of outsourced personnel and outsourced projects into the daily responsibilities of employees and projects. HUAWEI CLOUD 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.	The customer is responsible for developing the supplier monitoring strategy, including determining the monitoring indicators and monitoring frequency, and continuously monitoring the supplier according to the monitoring strategy. Monitor compliance with the organization's security processes and procedures based on the organization's information security requirements for suppliers. If an organization uses an external information system, it should also raise information security requirements and monitor the service provider of the external information system The Customer is responsible for regularly monitoring, reviewing and

				auditing the services provided by the Service Provider.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	ISO/IEC 27001:2013 A.12.4.1 A.14.2.7 A.15.2.1	Same as DE.AE-2 Same as DE.CM-6	Customer is responsible for monitoring their systems for unauthorized personnel, connections, equipment and software.

	DE.CM-8: Vulnerability scans are performed	ISO/IEC 27001:2013 A.12.6.1	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.	The customer is responsible for developing the vulnerability scanning process, including the target and frequency of scanning. Use vulnerability scanning tools and technologies to scan system vulnerabilities based on the vulnerability scanning process. Vulnerability scanning includes identifying platform and software vulnerabilities and misconfigurations, evaluating the impact of discovered vulnerabilities, forming vulnerability scanning reports based on the vulnerability scanning results, evaluating the risks of discovered vulnerabilities, and fixing vulnerabilities within a specified period of time.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	For each products and services' business units, the information security responsibilities of all employees and third-party stakeholders 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.	The customer is responsible for establishing the inspection process and clearly defining the roles and responsibilities of the inspection to ensure accountability.

	DE.DP-2: Detection activities comply with all applicable requirements	ISO/IEC 27001:2013 A.18.1.4 A.18.2.2 A.18.2.3	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. 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. HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for	The customer is responsible for ensuring that the testing process they develop meets the internal and external requirements of the organization.

			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.	

	DE.DP-3: Detection processes are tested	ISO/IEC 27001:2013 A.14.2.8	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.	The customer is responsible for conducting a safety assessment to verify the effectiveness of the safety inspection measures. The organization may conduct periodic penetration testing to verify that security monitoring is effective by bypassing or circumventing physical facility access and exit security controls without prior notice. Organizations can periodically verify the effectiveness of technical measures against malicious code attacks.

	DE.DP-4: Event detection information is communicated	ISO/IEC 27001:2013 A.16.1.2 A.16.1.3	HUAWEI CLOUD has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents. 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. HUAWEI CLOUD conveys the	The customer is responsible for communicating the results of the incident detection to both internal and external stakeholders.

			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.	

	DE.DP-5: Detection processes are continuously improved	ISO/IEC 27001:2013 A.16.1.6	Same as DE.AE-4	The customer is responsible for continually maintaining and reviewing security testing, training and monitoring plans to ensure that they comply with the organization's risk management strategy and prioritization of risk response activities.

5.4 Respond

Category	**Subcategory**	**Informative** **References**	**HUAWEI CLOUD's** **Response**	**Customer's Responsibilities**

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident	ISO/IEC 27001:2013 A.16.1.5	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	The customer is responsible for formulating the emergency plan, including the policy and process for responding to an information system interruption, intrusion, or fault, and initiating the emergency plan to respond to the event when the information system interruption, intrusion, or fault occurs. The customer is responsible for developing a security incident response plan, specifying the reporting and response processes of different security incidents, and responding to security incidents based on the developed processes.

			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.	

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2 A.16.1.1	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. 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. HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate.	The customer is responsible for training relevant personnel to ensure they understand their responsibilities and appropriate actions in incident response.

	RS.CO-2: Reported events meet established criteria	ISO/IEC 27001:2013 A.6.1.3 A.16.1.2	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. HUAWEI CLOUD is designated with dedicated personnel to	The customer is responsible for reporting events to internal and external stakeholders. Additionally, The customer is required to support investigations by relevant law enforcement agencies, as appropriate.

			maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies.	
	RS.CO-3: Information is shared consistent with response plans	ISO/IEC 27001:2013 A.16.1.2 Clause 7.4	Same as RS.CO-2 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 security incident response process defines the notification mechanism based on different types and levels of security incidents, including the notification mode, notification time, notification object, and notification content template.	The customer is responsible for developing a security event reporting mechanism, defining the types of security events to be reported, specifying the reporting process of different security events, and specifying the management responsibilities of security event reporting. Different reporting procedures shall be adopted for major security events that cause system interruption and information leakage.

	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	ISO/IEC 27001:2013 Clause 7.4	Same as RS.CO-3	When developing emergency plans and security incident response plans, the customer shall identify the internal and external stakeholders on which emergency response and security incident response activities depend, and specify the cooperation mode and process with all stakeholders.

	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	ISO/IEC 27001:2013 A.6.1.4	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 to work closely with external stakeholders to share information with a view to promoting progress in the cybersecurity field.	The customer should strengthen cooperation and communication with cybersecurity management departments, suppliers, industry experts, and security organizations to continuously enhance security education and training for organization personnel, keep a good understanding of excellent security practices and technologies, and share security information about new threats, vulnerabilities, and events. In addition, we shall establish a cybersecurity complaint and reporting system, publicize the information such as the complaint and reporting method, and promptly accept and handle the complaints

				and reporting related to cybersecurity.
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	ISO/IEC 27001:2013 A.12.4.1 A.12.4.3 A.16.1.5	Same as RS.RP-1 HUAWEI CLOUD has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents.	The customer analyzes and collects statistics on logs, detections, and alarms, discovers possible security events, and obtains event information to quickly respond to events.
	RS.AN-2: The impact of the incident is understood	ISO/IEC 27001:2013 A.16.1.4 A.16.1.6	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.	When an emergency occurs, the customer is responsible for determining the impact and level of the incident based on the security incident classification standards developed by the organization.

	RS.AN-3: Forensics are performed	ISO/IEC 27001:2013 A.16.1.7	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.	The customer is responsible for collecting evidence and documenting the handling process during the security incident reporting and response process. The information system should provide the capability of generating audit reports to support the investigation of security incidents and ensure that the audit records and timestamps cannot be tampered with.

	RS.AN-4: Incidents are categorized consistent with response plans	ISO/IEC 27001:2013 A.16.1.4	HUAWEI CLOUD has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents, and grade and handle the incident based on the incident response process.	The customer is responsible for formulating the classification and grading standards for information security incidents and specifying the corresponding response processes for incidents of different levels. When an information security incident occurs, the category and level of the incident should be determined based on predefined criteria so that corresponding countermeasures can be initiated.

	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	N/A	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 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.	The customer is responsible for continuously receiving information security alerts from external organizations designated by the organization, generating appropriate internal security alerts, and releasing them to external organizations, internal personnel, or roles designated by the organization. The customer should establish and maintain contact with relevant security organizations and associations in the industry to share the latest security threats, vulnerabilities, and incidents, as well as other security information.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident	RS.MI-1: Incidents are contained	ISO/IEC 27001:2013 A.12.2.1 A.16.1.5	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-	The customer is responsible for taking emergency measures to prevent the incident from deteriorating according to the developed incident handling mechanism and process, when an information security incident occurs, When the application software provided by the organization is found to contain malicious programs, the organization shall stop providing services and take measures such as elimination.

			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. 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 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 annually tests information security incident management procedures. All of information security incident response personnel, including reserve	

			personnel, need to participate.	
	RS.MI-2: Incidents are mitigated	ISO/IEC 27001:2013 A.12.2.1 A.16.1.5	Same as RS.MI-1	When an information security incident occurs, the customer is responsible for handling the incident according to the developed incident handling mechanism and process to minimize the impact of the incident.

	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	ISO/IEC 27001:2013 A.12.6.1	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.	The customer is responsible for timely remedying the discovered security vulnerabilities and hidden dangers, including taking measures to deal with the security problems found during the evaluation and monitoring of security control measures, and recording and taking risk handling measures for the risks identified during risk assessment. Assess the risks of vulnerabilities found during system vulnerability scanning and fix the vulnerabilities within the specified time.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities.	RS.IM-1: Response plans incorporate lessons learned	ISO/IEC 27001:2013 A.16.1.6 Clause 10	Same as RS.AN-2	The customer is responsible for including experience summary in the emergency plan framework to summarize the problems encountered during the implementation or test of the response procedure in the emergency plan, and incorporate the lessons learned into the response procedure of the emergency plan.
	RS.IM-2: Response strategies are updated	ISO/IEC 27001:2013 A.16.1.6 Clause 10	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.	Client is responsible for updating emergency response procedures to accommodate changes in organizational, information systems or operating environments or to resolve problems encountered during implementation or testing of emergency response procedures.

5.5 Recover

Category	Subcategory	Informative References	HUAWEI CLOUD's Response	Customer's Responsibilities
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	ISO/IEC 27001:2013 A.16.1.5	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 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.	The customer is responsible for formulating emergency plans and security incident response processes. The customer should formulate data backup policies, restoration policies, backup procedures, and restoration procedures based on data importance and impact on system running.

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities	RC.IM-1: Recovery plans incorporate lessons learned	ISO/IEC 27001:2013 A.16.1.6 Clause 10	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.	The customer is responsible for including the experience summary in the emergency plan framework to summarize the problems encountered during the implementation or test of the emergency plan response procedure, and incorporate the lessons learned into the emergency plan response procedure.

	RC.IM-2: Recovery strategies are updated	ISO/IEC 27001:2013 A.16.1.6 Clause 10	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. 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.	The customer is responsible for updating the recovery process in the contingency plan to adapt to changes in the organization, information system, or operating environment or to resolve problems encountered during the implementation or testing of the recovery process in the contingency plan.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed	ISO/IEC 27001:2013 A.6.1.4 Clause 7.4	HUAWEI CLOUD is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies. HUAWEI CLOUD has developed and implemented the proactive notification process to send service notifications that affect customer services to customers in a timely manner, so that customers can adjust service policies in a timely manner, reduce service impact, and improve customer experience.	The customer is responsible for establishing a crisis management mechanism, strengthening communication with the customer, the media, and the public, developing contingency plans for the public and the media, and promptly and accurately disclosing information in case of emergencies.

	RC.CO-2: Reputation is repaired after an incident	ISO/IEC 27001:2013 Clause 7.4	After a level-1 or level-2 incident occurs, the security incident contact person will synchronize with the public opinion contact person to initiate the crisis PR handling.	The customer is responsible for developing the communication strategy, method, principle, and plan with key stakeholders in advance. When an event occurs, the customer communicates with different stakeholders based on the communication strategy and plan to reduce or eliminate the negative impact of the event on the brand reputation of the organization.
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	ISO/IEC 27001:2013 Clause 7.4	Same as RC.CO-1	The customer is responsible for establishing a crisis handling mechanism, strengthening communication with the customer, media, and the public, developing contingency plans for the public and media, and promptly and accurately disclosing information in case of emergencies.

6 How HUAWEI CLOUD Helping Customers in Building a Cybersecurity System Based on the NIST CSF

HUAWEI CLOUD has passed the highest level certification of the NIST CSF and provides secure and reliable cloud services worldwide. HUAWEI CLOUD products and services can help customers with some of the five core functions of the NIST CSF and help them resolve cybersecurity risks. For details about the products, please refer to the **Product Page** on the HUAWEI CLOUD official website.

Function	Products Provided by HUAWEI CLOUD	Function Description
Identify	Data Security Center (DSC)	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.
	Compliance Compass (Compass)	Compass is a security compliance assessment and governance platform. Based on Huawei's experience in global security compliance, Compass offers security governance templates to help you comply with PCI DSS, ISO 27701, ISO 27001, and more. It automatically checks your services against preset compliance policies, intuitively presents your service compliance status, and allows you to quickly download compliance reports.

	Host Security Service (HSS)	Customers can 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.
	Vulnerability Scan Service (VSS)	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.
Protect	Identity and Access Management (IAM)	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 disoperation of a single user, and ensuring service continuity.

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

	Key Management Service (KMS)	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.
	SSL Certificate Manager (SCM)	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.

	Anti-DDoS	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.
	Object Storage Service (OBS)	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.
	API Gateway (APIG)	API Gateway is a high-performance, high-availability, and high-security API hosting service that helps you build, manage, and deploy Application Programming Interfaces (APIs) at any scale. With just a few clicks, you can integrate internal systems, monetize service capabilities, and selectively expose capabilities with minimal costs and risks. API Gateway helps you monetize service capabilities and reduce R&D investment, and enables you to focus on core enterprise services to improve operational efficiency. To monetize your service and data capabilities, you can open them up by creating APIs in API Gateway. Then you can provide the APIs for API callers using offline channels. You can also obtain open APIs from API Gateway to reduce your development time and costs.
	DevCloud	DevCloud is a one-stop, cloud-based DevOps platform. These out-of-the-box cloud services enable you to manage projects, host code, run pipelines, and build, deploy, and release your applications in the cloud anytime, anywhere.

	Cloud Trace Service (CTS)	Cloud Trace Service (CTS) is a log audit service for Huawei cloud security. It allows you to collect, store, and query resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.
Detect	Web Application Firewall (WAF)	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.
	Managed Threat Detection (MTD)	Managed Threat Detection (MTD) continuously checks source IP addresses and domain names in cloud service logs and alert you to potential malicious activities and unauthorized behaviors. MTD can monitor logs of IAM, DNS, CTS, and OBS, all of which are global services in your account. Powered by an AI engine, threat intelligence, and detection policies, MTD intelligently examines access behavior in logs of cloud services to detect threats, generate alarms, and provide remediation. With MTD, you can respond to alarms, handle potential threats, and harden service security in a timely manner to prevent major losses such as information leakage, keeping your accounts and service secure and stable.
	Situation Awareness (SA)	Situation Awareness (SA) is a GUI-based security event management and situation analysis platform on HUAWEI CLOUD. SA comprehensively analyzes attack events, threat alarms, and attack sources by leveraging the big data technique, making it simple for you to understand security situation across all your cloud assets.

	Log Tank Service (LTS)	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.
	Cloud Eye Service (CES)	Customers can use Cloud Eye Service (CES) provided by HUAWEI CLOUD to monitor utilization of ECS resources and network bandwidth in a multidimensional 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.
	Simple Message Notification (SMN)	Simple Message Notification (SMN) is a reliable and flexible large-scale message notification service. It enables you to efficiently send messages to phone numbers, email addresses, and HTTP/HTTPS servers, and connect cloud services through notifications, reducing system complexity.
Recovery	Cloud Server Backup Service (CSBS)	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.
	Cloud Backup and Recovery (CBR)	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.

7 Conclusion

HUAWEI CLOUD always adheres to HUAWEI's “customer-centric” core values and commit to protect customers data security resulting in the establishment of an information security management system and the deployment of the most common data security protection technologies in the industry to ensure customers data security.

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

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

8 Version History

Date	Version	Description
2022-02	1.0	First Publication