HUAWEI CLOUD User Guide to C-RAF 2.0 in Hong Kong Special Administrative Region of the People's Republic of China

Issue	1.0
Date	2022-09-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Background and Purpose of Publication

The rapid development of information technology has brought significant benefits to financial institutions in Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong SAR, China), but it has also created a complex environment for financial institutions. To strengthen the ability of Hong Kong's financial system to cope with cybersecurity risks, the Hong Kong Monetary Authority (HKMA) published the Cybersecurity Fortification Initiative (CFI). Financial institutions (authorized institutions, AIs) in Hong Kong SAR, China are required to implement the Cyber Resilience Assessment Framework (C-RAF).

As a cloud service provider, HUAWEI CLOUD is committed to assisting financial customers to meet these regulatory requirements and continuously providing financial customers with cloud services and business operation environment that comply with the regulatory requirements of the financial industry. The purpose of this white paper is to focus on the maturity assessment of C-RAF 2.0, and to describe in detail how HUAWEI CLOUD will assist financial institutions in Hong Kong SAR, China to meet the relevant control principles specified in the maturity assessment matrix of C-RAF 2.0 when using cloud services.

1.2 Introduction of C-RAF 2.0

The Hong Kong Monetary Authority (HKMA), who is the primary of the financial industry in Hong Kong SAR, China. In order to further strengthen the cybersecurity capability of AIs in Hong Kong SAR, China, HKMA published the Cybersecurity Fortification Initiative (CFI) on May 24, 2016 and issued the implementation details of CFI on December 21, 2016. CFI consists of the following three pillars:

- Cyber Resilience Assessment Framework (C-RAF): It is a risk-based framework for AIs to assess their own risk profiles, develop and implement appropriate defense measures against cyber-attacks.
- Professional Development Programmer (PDP): It develops certification programs and professional training courses for cybersecurity practitioners to train professional cybersecurity practitioners for the financial industry and even the information technology industry.

- Cyber Intelligence Sharing Platform (CISP): It provides an effective infrastructure for sharing intelligence on cyber-attacks. AI can receive prompt or warning from the cyber intelligence-sharing platform in time to respond to possible cyber-attacks in the financial industry.

Among them, C-RAF contains three parts:

- Inherent Risk Assessment: AIs can assess their own inherent cybersecurity risk level and determine their expected maturity level through an assessment matrix including five categories (technologies, delivery channels, products and technology services, business size and organizational characteristics, track record of cyber threats).
- Maturity Assessment: AIs can assess their current cybersecurity maturity level through a maturity assessment matrix including 26 components in seven fields, and determine whether there are gaps with the expected maturity level. AIs will develop a plan to improve their maturity level if there are gaps.
- Intelligence-led Cyber Attack Simulation Testing (iCAST): It is a test of AI cybersecurity capability simulates real cyber-attacks from adversaries by using relevant cyber intelligence. AI whose inherent risk level is assessed as "intermediate" or "advanced" should be iCAST within a reasonable time.

AIs had largely completed one round of their C-RAF assessments by late 2019 i.e., CRAF1.0. In the light of that and recent international developments in cybersecurity, the HKMA conducted a holistic and independent review of the CFI. Considering the experience gained in the past few years, the feedback received from industry consulting, overseas developments and new practices, HKMA revised CFI and released CFI 2.0 and C-RAF 2.0 on November 3, 2020 (effective January 1, 2021).

C-RAF 2.0 is a structured assessment framework. Through this framework, AIs can assess their inherent risks and maturity level of cybersecurity measures according to a set of "control principles". Through this process, AIs should be able to better understand, assess, strengthen and continuously improve their cyber resilience.

In order to comply with C-RAF 2.0, AIs are required to assess and ascertain its inherent risk rating through performing an Inherent Risk Assessment. The inherent risk rating is then mapped to its respective maturity level of cyber resilience. Based on their maturity level of cyber resilience, AIs should assess and determine the actual maturity level of its cyber resilience by performing the Maturity Assessment. Any gap between the expected maturity level and the actual maturity level should be marked as needing improvement, so that AIS can further enhance their cybersecurity and achieve the maturity expected by the HKMA. For AIs aim to attain the "intermediate" or "advanced" maturity level are required to conduct the iCAST, where AIs are required to apply a risk-based approach to identify the attack scenarios relevant to their institution, and ensure they are tested under the iCAST exercise to simulate real-life attacks conducted by competent adversaries.

According to the requirements of HKMA, the assessment of C-RAF should be generally conducted on a three-year frequency basis. AIs should proactively evaluate whether more frequent assessments are needed considering such factors as their inherent risk rating, changes to the AI's business nature or adopted technologies. By using a risk-based approach, AIs rated with high inherent risk should consider assessment with a review cycle of less than three years.

1.3 Definitions

- **HUAWEI CLOUD**

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

- **Service provider**

  An entity, including its branches providing services to a FI under an outsourcing arrangement.

- **Cloud computing**

  Cloud computing refers to a type of internet-based computing that provides shared computer processing resources and data on demand according to the National Institute of Standards and Technology (NIST).

- **Cyber resilience**

  The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

2 HUAWEI CLOUD Certification

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of international and industry security compliance certifications, ensuring the security and compliance of businesses deployed by cloud service customers.

HUAWEI CLOUD has attained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.

Certification	Description
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC Audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
CSA STAR Gold Certification	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.

Certification	Description
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
M&O Certification	Uptime Institute is a globally recognized data center standardization organization and authoritative professional certification organization. HUAWEI CLOUD data center has adopted the world's top data center infrastructure O&M certification (M&O certification) issued by Uptime Institute. The adoption of M&O certification indicates that HUAWEI CLOUD data center O&M management is at the leading level in the world.
NIST CSF	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.
PCI 3DS Certification	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.

Regional standard certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	Cloud service user data protection capability evaluation is a mechanism for evaluating the security of cloud service user data. Key indicators include pre-event prevention, in-event protection, and post-event tracing.
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) (China)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. HUAWEI Cloud has obtained cloud computing service capability level-1 (top level) compliance certificates.
Trusted Cloud Assessment	Trusted Cloud Assessment is an authoritative evaluation of cloud computing services and products organized by the Data Center Alliance (DCA) and the Telecom Research Institute of the Ministry of Industry and Information Technology (China Academy of Information and Communications Technology (CAICT)).

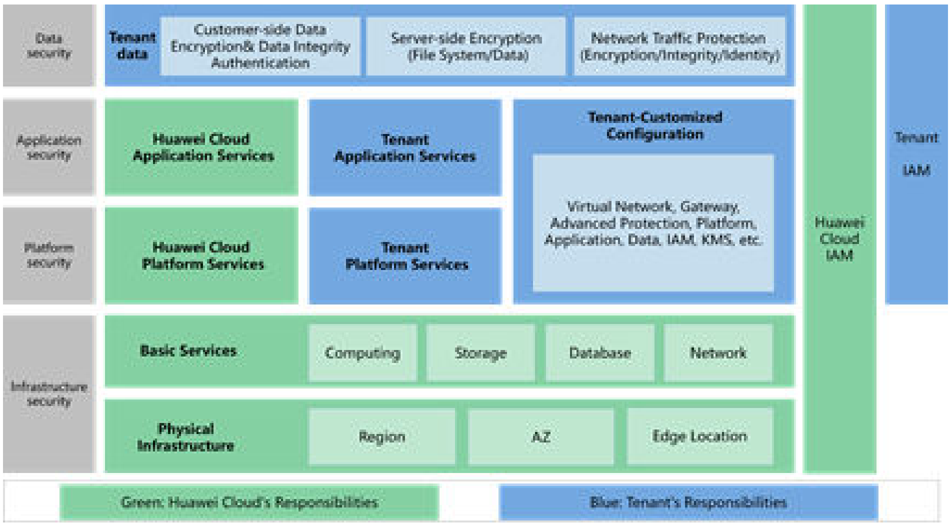
Certification	Description
Cyber Security Review by the Office of Cyber Security	Cyber security review by the Office of Cyber Security is a third-party security review conducted by the Office of the Central Cyberspace Affairs Commission according to the national standard Cloud Computing Service Security Capability Requirements. The HUAWEI CLOUD e-Government cloud platform successfully passed the security review (enhanced level), indicating that the Huawei e-Government cloud platform is recognized by the national cyber security management organization in terms of security and controllability.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance certificate, please refer to the official website of HUAWEI CLOUD **"Trust Center - Compliance Center"**.

3 HUAWEI CLOUD Security Responsibility Sharing Model

Due to the complex cloud service business model, cloud security is not the sole responsibility of one single party, but requires the joint efforts of both the customer and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenant 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 3-1 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
Huawei Cloud IAM
Tenant IAM
Infrastructure security
Basic Services
Computing
Storage
Database
Network
Physical Infrastructure
Region
AZ
Edge Location
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 services 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.

4 HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD **"Worldwide Infrastructure"**.

5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of C-RAF 2.0

C-RAF 2.0 was established to minimize repetitive and disruptive actions and to assist AIs in identifying control gaps and developing cyber resiliency remediation and enhancement actions to reduce cybersecurity risk. The maturity assessment matrix of C-RAF 2.0 provides control objectives and principles for AI to achieve the corresponding cybersecurity maturity level, including governance, identification, protection, detection, response and recovery, and situational awareness, and third-party risk management in a total of seven domains.

When AIs are seeking to comply with the requirements provided in the C-RAF 2.0 maturity assessment matrix, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the maturity assessment matrix of C-RAF 2.0, and explains how HUAWEI CLOUD, as a cloud service provider, can help AIs to meet these requirements.

**Remarks: "Customer Responsibility" in this chapter respectively describe the controls that AI customers need to implement at Low (Baseline), Medium (Intermediate), and High (Advanced) maturity levels.*

5.1 Identification

5.1.1 IT asset management

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
2.1.1	IT asset management	Low: the customer should establish an accurate and complete view of the operating environment to provide visibility of the holistic attack surface and facilitate the review of the adequacy and effectiveness of cyber control. Medium: in addition to the above controls, the customer should establish a process to update the IT asset inventory and prevent deviations without proper review and approval. High: in addition to the above controls, the customer shall establish controls to prevent unauthorized additions, changes or deviations to the IT asset baseline, thus restricting the possibility of unintended or malicious increases being made to the attack surface.	As a cloud service provider, in order to cooperate with customers to meet regulatory requirements: **Host Security Service (HSS)** of HUAWEI CLOUD provides a unified management interface for customers to query and manage cloud services. It is the security manager of servers and provides asset management functions for customers, including manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software. HUAWEI CLOUD has formulated asset management procedures, which specify the confidentiality and grading methods of information assets and the authorization rules that should be followed for various types of assets. In addition, HUAWEI CLOUD has established information asset confidentiality management requirements, which specify the confidentiality measures that HUAWEI CLOUD should take for information assets at different levels, and standardize the use of assets to ensure that the company's assets are properly protected and shared. HUAWEI CLOUD uses the Cloud Asset Management system to monitor the inventory and maintenance status of HUAWEI CLOUD information assets recorded on the asset management platform in real time, classify, monitor, and manage information assets, and generate an asset list for each asset. In addition, In HUAWEI CLOUD, configuration managers are assigned to manage the configuration of all services, the resource configuration model consists of hosts, service trees,

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			cloud infrastructures, and network devices. Configuration item mapping and resource lifecycle management are constructed to ensure stable and secure O&M in production environment. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes. HUAWEI CLOUD uses IPAM to centrally manage IP resources. In addition, the HSP host security platform suite is deployed on the HUAWEI CLOUD platform to provide cybersecurity protection for platform assets.

5.2 Protection

5.2.1 Access control

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.1.1	User account management	Low: the customer shall establish a user account management mechanism, manage the access rights of employees to the system and confidential data according to the principle of minimum permission and separation of duties, and implement appropriate password strategies and encryption functions, account locking strategies, permission application approval and review mechanisms. Medium: in addition to the above control, the customer shall establish a monitoring and alarm mechanism for user authority change, and a verification mechanism for password generation and modification with the common password library. High: in addition to the above control, the customer shall implement multi factor authentication for locally accessed non-privileged accounts based on risk considerations, and establish an access control	HUAWEI CLOUD provides **Identity and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication. IAM provides federation authentication for customers. Customers who have a reliable identity authentication service provider in place can map their federated users to IAM users in a specified period for access to customer's HUAWEI CLOUD resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. HUAWEI CLOUD has established Internal operation and maintenance account lifecycle management. It includes account management, account owner/user management, password management, account management monitoring, etc. Once created, new accounts are immediately scoped in for daily O&M by security administrators. All operation and maintenance accounts, accounts of all devices and applications are managed in a unified manner, and are centrally monitored through a unified audit platform, and automatic auditing is

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
		mechanism for collaborative computing devices and applications.	performed to ensure the full process management from user creation, authorization, authentication to permission recovery. If the account user wants to use the account, the account administrator can start the authorization process, and authorize by password or by increasing the authority of the account; the applicant and the approver of the account cannot be the same person. HUAWEI CLOUD implements role-based access control and permission management for internal personnel, restricting personnel with specified positions and responsibilities to only perform specified operations on authorized targets. Ensure that personnel do not gain unauthorized access through minimal privilege assignment and strict behavioral auditing. HUAWEI CLOUD has specified the maximum review period for accounts/ rights at specified 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. O&M: At the same time, when HUAWEI CLOUD O&M personnel access HUAWEI CLOUD Management Network for centralized management of the system, they need to use only identified employee identity accounts. In addition, two-factor authentication is used to authenticate cloud personnel, such as USB key, Smart Card and so on. Employee account is used to log on VPN and access gateway to realize the deep audit of user login. Privileged Account Management

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.1.2	Privileged user account managem ent	Low: the customer should establish a strict management mechanism for privileged accounts and implement multi factor authentication for privileged accounts. Medium: in addition to the above control, the customer shall establish a review mechanism for privileged users, apply multi factor authentication to high-risk systems, and enforce the principle of least privilege. High: in addition to the above controls, the customer shall establish an access control mechanism (if applicable) for collaborative computing devices and applications based on risk considerations to restrict the use of specific privileged commands.	System binds functional or technical accounts of daily or emergency operations to operation and maintenance teams or individuals. Strong log auditing is supported on the bastion host to ensure that the operation and maintenance personnel's operations on the target host can be located to individuals. Grant privileged or emergency accounts to employees only when necessary for their duties. All applications for privileged or emergency accounts are subject to multiple levels of review and approval.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.1.4	Physical access management	Low: the customer shall implement physical access management, restrict and log the physical access to high-risk or confidential systems such as hardware and telecommunication systems, continuously monitor the physical access, and regularly review the physical access log. Medium: N/A. High: N/A.	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. Security guards strictly review and regularly audit user access privileges. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system (WMS). Designated personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis to ensure that unauthorized personnel have no access to data centers.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.1.5	Remote access management	Low: the customer shall use encrypted connection and multi factor authentication for remote access of employees, contractors and third parties, and implement multi factor authentication for non-privileged accounts with network access rights. Medium: in addition to the above control, the customer shall implement encryption mechanism to protect the confidentiality and integrity of remote access, and route all remote access through the centrally managed network access control point to monitor remote access sessions and audit user activities. High: in addition to the above control, the customer shall authorize the execution of privileged commands and other sensitive operations through remote access as required and record and regularly review the reasons for access.	HUAWEI CLOUD employees use unique identity in the internal office network. If the external network needs to be connected to HUAWEI working network, it is necessary to access through VPN. For O&M scenarios, centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in HUAWEI CLOUD data centers. The data center external network operation and maintenance personnel and intranet operation and maintenance personnel centrally manage all local and remote operations of network, server and other equipment, and realize unified access, unified authentication, unified authorization, and unified auditing of equipment resource operation management by users. For remote management of HUAWEI CLOUD, whether from the Internet or office network, it is necessary to first access the resource pool bastion host, and then access related resources from a bastion server.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.1.8	Cryptographic keys management	Low: the customer shall establish encryption key management policies, procedures and control measures covering key generation, distribution, installation, renewal, revocation and expiration to prevent unauthorized access to encryption keys. Medium: N/A. High: N/A.	HUAWEI CLOUD provides **Key Management Service (KMS)**. It helps users to centrally manage keys and protect key security. It uses a Hardware Security Module (HSM) to create and manage keys for tenants, preventing the key plaintext from being exposed outside the HSM, thereby preventing key leakage. Currently, the following HUAWEI CLOUD services have been interconnected with the KMS service: **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Cloud Backup and Recovery (CBR)**, **Image Management Service (IMS)**. HUAWEI CLOUD formulates and implements cryptographic algorithm application specifications This document describes how to select secure encryption algorithms and the rules for using secure encryption algorithms. It also provides guidance on the correct use of cryptographic algorithms with application examples. HUAWEI CLOUD uses the AES encryption method widely used in the industry to encrypt data on the platform, and uses the high version TLS encryption protocol to secure data during the transmission processes, ensuring data confidential in different states. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.

5.2.2 Infrastructure protection control

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.2.1	Network protection	Low: the customer shall use the network peripheral defense tools to continuously monitor the high-risk network ports. Strong encryption (if applicable) is required for identity authentication and data transmission through the wireless network. Firewalls shall be deployed between the Internet access point and the DMZ area and the intranet, a mechanism for firewall rule change and regular audit shall be established, an intrusion detection/prevention system shall be deployed, and technical control shall be implemented to prevent unauthorized network connection. Medium: in addition to the above control, the customer shall partition the enterprise network and adopt the defense in depth strategy. Implement security control for remote access management console. Deploy peripheral firewalls for wireless networks and use high-strength encryption	HUAWEI CLOUD data center has many nodes and complex functional areas. To simplify network security design, prevent the spread of cyber-attacks on HUAWEI CLOUD, and minimize the impact of attacks, HUAWEI CLOUD divides and isolates security zones, services based on ITUE.408 security zone division principles, and best network security practices in the industry. Nodes in a security zone have the same security level. HUAWEI CLOUD network architecture design, device selection, configuration, and O&M are considered. HUAWEI CLOUD uses multiple layers of security isolation, access control, and border protection technologies for physical and virtual networks, and strictly implements management and control measures to ensure HUAWEI CLOUD security. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and cybersecurity risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD maintains the latest network topology. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, public service, POD-Point of Delivery, OBS-Object-Based Storage, and OM-Operations Management. In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
		keys. Physically isolate the guest wireless network from the intranet. Anti-spoofing measures are adopted to detect and block the forged source IP address from entering the network. High: in addition to the above control, the customer shall deploy tools and/or develop processes to block attempted access from unpatched employee-owned devices and unauthorized device, limit and monitor the traffic between trusted and untrusted zones, and regularly or as needed assess and review environmental changes, identify gaps and take a remediation plan.	to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. HUAWEI CLOUD isolates data on the cloud by using the **Virtual Private Cloud (VPC).** VPC uses the network isolation technology to isolate tenants at Layer 3 networks. Tenants can completely control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using **Virtual Private Network (VPN)** or **Direct Connect (DC)**, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configuration security and access rules on demand to meet tenants' fine-grained network isolation requirements. In terms of network border protection, HUAWEI CLOUD has established a solid and complete border and multi-layer security protection system, and deployed Anti-DDoS, IDS/IPS, and WAF protection mechanisms. Anti-DDoS quickly detects and defends against DDoS attacks and comprehensively defends against traffic attacks and application-layer attacks in real time. WAF detects and defends against web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately. The IDS/IPS detects and blocks cyber-attacks from the Internet in real time and monitors abnormal host behaviors.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.2.2	System configuration	Low: the customer shall establish and implement the system security configuration baseline to monitor the system configuration changes. Medium: in addition to the above control, the customer shall regularly review the Critical systems to identify potential vulnerabilities, upgrade opportunities or new defense layers, and control and regularly test the unsupported systems to validate their effectiveness. High: in addition to the above control, the customer shall establish appropriate control measures to prevent the execution of unauthorized code on owned or managed devices, and systems components.	HUAWEI CLOUD hardens the security configurations of host operating systems, VMs, databases, web application components, and allows customers to select appropriate security configurations based on their service requirements. For example, in terms of host security, the host OS uses Huawei Unified Virtualization Platform (UVP) to manage CPU, memory, and I/O resources in isolation. The host OS has been minimized and service security has been hardened. In terms of VM security, HUAWEI CLOUD provides security configurations such as image hardening, network and platform isolation, IP/MAC spoofing control, and security groups.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.2.3	Virtualization security	Low: the customer shall formulate policies for managing the security, creation, distribution, storage, use, retirement and destruction of virtual machine images and snapshots, and implement control measures for administrative access to the hypervisor and host operating system. Medium: N/A. High: N/A.	HUAWEI CLOUD adopts a series of security mechanisms for VMs to cope with cybersecurity risks. The VM security of HUAWEI CLOUD isolates the network from the platform. On the network layer, a virtual switch provided by the hypervisor on each host is used to configure VLAN, VXLAN, and ACL settings to ensure that the VMs on that host are logically isolated. UVP supports the configuration of security groups to isolate VMs by group. Tenants can create security groups containing multiple VMs to enable those VMs to access each other while maintaining isolation from other VMs. By default, VMs in the same security group can access each other but any two VMs in different security groups cannot access each other. That said, the tenant could also customize access and communication between any two VMs in different security groups. HUAWEI CLOUD's professional security team performs security hardening on public images and patches any system vulnerabilities that may occur. Secure, updated public images are created with the help of an image factory and provided to users through **Image Management Service (IMS)**. Pertinent hardening and patch information is provided to tenants for reference during image testing, troubleshooting, and other O&M activities. When creating VMs, tenants can decide based on their applications and security policies whether to use an up-to-date public image or create a private image that has the required security patches installed.

5.2.3 Data protection

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.3.2	Data protection	Low: the customer shall specify the standards and requirements for data encryption, encrypt the confidential data transmitted in the public or untrusted network, encrypt the confidential data stored on the mobile device, desensitize the customer's data in the non-production environment, and formulate policies and procedures for data disposal and destruction. Medium: in addition to the above controls, the customer shall use tools to prevent and/or detect unauthorized access to or exfiltration of confidential data. High: in addition to the above control, the customer shall encrypt the confidential data transmitted in transit across private connections and within the trusted zones.	HUAWEI CLOUD uses a series of protection mechanisms to protect tenant data storage security. First, HUAWEI CLOUD provides **Key Management Service (KMS)**. It helps users to centrally manage keys and protect key security. It uses a Hardware Security Module (HSM) to create and manage keys for tenants, preventing the key plaintext from being exposed outside the HSM, thereby preventing key leakage. Currently, the following HUAWEI CLOUD services have been interconnected with the KMS service: **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Cloud Backup and Recovery (CBR)**, **Image Management Service (IMS)**. Second, the storage and database services provided by HUAWEI CLOUD are guaranteed to be highly reliable. For example, EVS cloud hard disk uses a multi-copy data redundancy protection mechanism, and adopts measures such as synchronous write and read recovery of copies to ensure data consistency. When hardware failure is detected, it can be automatically repaired in the background, data is quickly and automatically rebuilt, and data durability can reach 99.9999999%; OBS object storage service supports the high reliability of object data, and through the high reliability network of business nodes and the multi-redundancy design of nodes, the system design availability reaches 99.995%, which fully meets the high availability requirements of object storage services. Provides multiple redundancy of object data and automatic restoration technology

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			to ensure the data consistency of multiple objects to provide high reliability of object data. The system design data durability is as high as 99.9999999999%; RDS relational database service adopts hot standby architecture, failure system 1 minute automatic switching. Data is automatically backed up every day, uploaded to the OBS bucket, and the backup files are retained for 732 days. One-click recovery is supported. For the data in transit, the data from the client to the server and between the servers on the HUAWEI CLOUD platform is transmitted through a public information channel. The protection of the data in transit is through **Virtual Private Network (VPN)** and application layer TLS and certificate management. , HUAWEI CLOUD services provide customers with two access methods: console and API. Both use encrypted transmission protocols to build secure transmission channels, effectively reducing the risk of malicious sniffing of data during network transmission. For data security deletion, after the customer confirms the deletion of data, HUAWEI CLOUD will comprehensively clear the specified data and all its copies. First, delete the index relationship between the customer and the data, and then delete the storage space such as memory and block storage. Perform a clearing operation before reallocation to ensure that the related data and information cannot be restored. When the physical storage medium is scrapped, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			ensure that the data on it cannot be recovered.

5.2.4 Secure development

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.4.1	Secure development	Low: the customer shall establish the management framework and policies of the System Development Life Cycle (SDLC) and embed the security requirements such as access control, authentication, authorization, data integrity and logging in all phases of SDLC. Medium: in addition to the above control, the customer shall formulate and implement the safety standards at all stages, establish the defect management process, and conduct the safety test on the application connected to the Internet. High: in addition to the above control, the customer shall establish and strictly implement the change and release management process, fully review the dependency between applications and services, identify vulnerabilities through code reviews and/or static code analyses, and conduct security tests on applications.	HUAWEI CLOUD implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, etc. HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services. HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. Before they are on boarded, HUAWEI CLOUD service development and test personnel are all required to learn corresponding specifications and prove they have learned these by passing examinations on them. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/ Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code related issues that can extend rollout time coding.

5.2.5 Patch and change management

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.5.1	Patch management programme	Low: the customer shall implement patch management procedures and ensure that software and firmware patches are applied in time. Medium: in addition to the above control, the customer identifies the missing security patches and the available days of the patches through tools and/or processes. High: in addition to the above control, the customer shall install patch monitoring software covering all servers, review patch management reports, and timely test and install security patches.	HUAWEI CLOUD establishes a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. In addition, HUAWEI CLOUD has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services, continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.5.2	Patch assessment and testing	Low: the customer shall establish a formal process for obtaining; testing and deploying patches based on critical software, and test the patches before applying them to the system/ software. Medium: in addition to the above control, the customer should conduct impact assessment before deploying security patches, maintain and regularly review existing vulnerabilities, and report to the management regularly. High: in addition to the above control, the customer should use automation and categorization technology measures to facilitate large-scale and rapid patch repair.	HUAWEI CLOUD uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In addition, HUAWEI CLOUD has established a security vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability handling requirements. In addition, HUAWEI CLOUD has established a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.5.3	Change management process	Low: the customer shall formulate the change management process and implement the change application and approval mechanism. Medium: in addition to the above control, the customer shall evaluate the cybersecurity risk during the implementation of the change, assign appropriate personnel to be responsible for the change approval, and formal change request, documented approval and security impact assessment are required for the changes to the baseline IT configuration. High: in addition to the above control, the customer shall implement a change management system and use tools to detect and block unauthorized changes.	HUAWEI CLOUD has developed change management regulations and change processes, which define cyber security requirements that must be followed before, during, and after change implementation to prevent unauthorized changes. For example, before a change, all changes need to be reviewed in multiple phases. During the change implementation, log recording, operation monitoring, and two-person operation are used to ensure the security of the change implementation and ensure that the change process is traceable. After the change, assign personnel to verify the change to ensure that the change achieves the expected effect and does not cause cyber security risks. After all change requests are generated, they are submitted to the HUAWEI CLOUD Change Committee by the change manager team with change classification assigned. After the committee has reviewed and approved the requests, the planned changes can be implemented on the production network. 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.

5.2.6 Remediation management

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
3.6.1	Remediation management	Low: the customer shall establish a repair management process to repair the identified problems in time. Medium: in addition to the above control, the customer shall establish a repeated simulation test mechanism to ensure that medium and high-risks exploitable vulnerabilities are solved. High: in addition to the above control, the customer shall establish an authorization and approval mechanism for asset maintenance and repair, and timely record and review the maintenance and repair of the organization's assets. For key and high-risk issues that cannot be solved in time, appropriate mitigation measures shall be taken and reported to the management.	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. At the same time, customers can use HUAWEI CLOUD **Host Security Service (HSS)** to detect vulnerabilities in the Windows and Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provides fixing suggestions. At the same time, customers can use HUAWEI CLOUD Host Security Service (HSS) to detect vulnerabilities in the Windows and Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provides fixing suggestions. In addition, HUAWEI CLOUD can provide customers with a **Container Guard Service (CGS)** that can scan vulnerabilities and configuration information in images, helping enterprises resolve container environment problems that cannot be detected by traditional security software. HUAWEI CLOUD has established a security vulnerability management process, which standardizes the closed-loop process of early warning, assessment, and repair processing of HUAWEI CLOUD system security vulnerabilities, ensures the regular installation of critical security patches HUAWEI

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			CLOUD has established a security vulnerability management process, which standardizes the closed-loop process of early warning, assessment, and repair processing of HUAWEI CLOUD system security vulnerabilities, ensures the regular installation of critical security patches company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed. In addition, HUAWEI CLOUD is equipped with dedicated personnel to maintain contact and establish contact points.

5.3 Detection

5.3.1 Vulnerability detection

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.1.1	Antivirus and anti-malware	Low: the customer should deploy automatically updated antivirus and anti-malware tools, and implement email protection mechanism to filter for common cyber threats. Medium: in addition to the above control, the process and tools implemented by the customer (such as sandbox) conduct behavior analysis to detect and block the existing malware. High: in addition to the above control, the customer shall establish a centralized and automatic terminal protection mechanism.	Customers can use the **Host Security Service (HSS)** of HUAWEI CLOUD, by detecting program features and behaviors and using the AI image fingerprint algorithm and cloud-based virus scanning and removal, the system can effectively identify malicious programs, such as viruses, Trojan horses, backdoors, worms, and mining software, and provide one-click isolation and virus removal capabilities. 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. At the physical host level, antivirus software is deployed to achieve defense against malware attacks. Anti-virus software is provided by default within the standard image of HUAWEI CLOUD Desktop Terminal, and employees cannot disable the anti-virus software. HUAWEI CLOUD has implemented comprehensive malware and virus protection mechanisms for the cloud platforms. HUAWEI CLOUD uses IPS intrusion prevention system, Web Application Firewall

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			(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 figurations 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.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.1.2	Penetration/ Simulation Testing	Low: the customer should conduct penetration testing and vulnerability scanning regularly. Medium: in addition to the above control, the customer shall conduct simulation tests regularly or after major changes. The customer should continuously conduct vulnerability scanning to ensure that all high-risk systems are covered throughout the year. High: in addition to the above control, the customer establishes a vulnerability scanning process covering all terminals.	HUAWEI CLOUD has established a periodic vulnerability scanning mechanism, and implements monthly vulnerability scanning for products within the scope of the report, and the vulnerability scanning team is responsible for tracking and processing the scanning results. HUAWEI CLOUD will organize internal and external qualified third parties to scan all HUAWEI CLOUD systems, applications and networks for vulnerabilities every quarter. In addition, HUAWEI CLOUD organizes internally or external third parties with certain qualifications to conduct penetration tests on all HUAWEI CLOUD platform systems within 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.

5.3.2 Anomalies activity detection

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.2.1	Log monitoring and analysis	Low: the customer establish processes, control measures to timely, and accurately detect abnormal security behaviors. Medium: in addition to the above control, the customer shall back up the audit logs to the centralized log server to prevent unauthorized changes to the logs. High: N/A.	**Log Tank Service (LTS)** on HUAWEI CLOUD collects, queries, and stores logs in real time. Its records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. **Cloud Eye Service (CES)** is a comprehensive monitoring platform for Elastic Cloud Servers, bandwidth, and other resources. Customers can monitor user login logs in real time. When malicious login occurs, an alarm is generated and the requests from the IP address are rejected. HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information. 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

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			data analytics can quickly collect, process, and analyze mass logs in real time.
4.2.2	Security information and event management	Low: the customer shall establish processes and controls to alert a designated security function to investigate abnormal behavior. Medium: in addition to the above control, the customer should deploy tools to detect unauthorized data mining and actively monitor security logs. High: in addition to the above control, the customer shall use the system to monitor and analyze employee behavior, implement measures to monitor sensitive data or files, and use defense-in-depth techniques to detect and respond to cyber-attacks in a timely manner.	To ensure the professionalism, urgency, and traceability of security event handling, HUAWEI CLOUD has comprehensive security log management requirements, security event rating and handling processes, a 24/7 professional security event response team, and a corresponding security expert resource pool. HUAWEI CLOUD strives to achieve rapid security incident response in terms of incident detection, impact scoping, damage isolation, and service recovery. In addition, HUAWEI CLOUD keeps our security event rating criteria, time to response, and time to resolution up to date by considering the impact of a security event or incident on our entire network and customers.

5.3.3 Cyber incident detection

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.3.1	Event monitoring	Low: the customer shall establish an event monitoring mechanism and assign responsibilities for monitoring and reporting events. Medium: in addition to the above control, the customer shall establish a normal network activity baseline to monitor the safety of critical assets. High: in addition to the above controls, the customer should implement processes and solutions for evaluating malicious behavior /software.	HUAWEI CLOUD log analysis platform collects security logs of operation systems, servers, and network devices. In addition, the platform presets abnormal operation rules to identify abnormal operations, automatically generates alarms, and pushes the alarms to security departments for follow-up processing. Abnormal alarms are handled in a timely manner according to service level agreements, and screen monitoring and recording through the incident analysis and processing platform in real-time. HUAWEI CLOUD security incident response team is responsible for incident monitor and record, and assess whether a security incident is, also they track and manage the collected security incident by unified management to ensure security incident can be fixed in time. Moreover, HUAWEI CLOUD regularly conducts statistics and trend analysis of incidents. For similar incidents, the problem handling team will find the root causes and formulate solutions to prevent such incidents from occurring.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.3.2	Detection and alert	Low: the customer shall establish event detection and alarm mechanism, deploy tools, set appropriate alarm parameters, and risk indicators to detect, alert and trigger event response programme Medium: in addition to the above control, the customer shall detect events in real time through automated processes and provide sufficient resources to achieve continuous detection, investigation, analysis and response. High: in addition to the above control, the customer shall install automatic tools to detect unauthorized changes to critical system files and security equipment, and implement real-time network monitoring and detection tools.	

5.3.4 Threat monitoring and analysis

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
4.4.1	Threat monitoring and analysis	Low: the customer shall develop a monitoring process for Threat Intelligence. Medium: in addition to the above control, the customer shall clarify the responsibility of Threat Intelligence Monitoring and analysis, establish a Security Operation Centre, and continuously monitor the threat situation. High: in addition to the above control, the customer shall conduct Threat Intelligence Analysis and report formulation to determine follow-up actions. Use threat intelligence to update the organization's IT security architecture and its configuration standards, and predict potential attacks and attack trends.	As a cloud service provider, in order to cooperate with customers to meet regulatory requirements: **Managed Threat Detection (MTD)** of HUAWEI CLOUD continuously detects whether the IP or domain name of the visitor in the IAM log, DNS log, CTS log, OBS log and VPC log generated by the user's operation in HUAWEI CLOUD in the target area is subject to potential malicious activities and unauthorized behaviors. If any abnormality is found, a timely alarm will be given. This service integrates three capabilities of AI intelligent engine, Threat Intelligence and rule baseline to realize threat detection. It intelligently detects abnormal access behaviors implied in log data from multiple cloud services (including IAM service, DNS service, CTS service, OBS service and VPC service), proactively finds potential threats, generates alarm information for access behaviors that may have threats, and outputs alarm results. The user can check and process the alarm information through the alarm description, and timely deal with the potential threats before causing major losses such as information leakage, and upgrade and reinforce the service security, to protect the user's account security and ensure the stable operation of the service. **Situation Awareness (SA)** is a security management and situation analysis platform provided by HUAWEI CLOUD. It detects multiple cloud security risks, including DDoS attacks, brute force cracking, web attacks, backdoor Trojan horses, zombie hosts, abnormal behaviors, vulnerability attacks, and command

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			and control. With big data analytics, SA can classify and analyze attack events, threat alarms, and attack sources. This helps customers identify, collect, obtain evidence about information security events, and analyze events to reduce the possibility and impact of events in the future. In addition, SA can be associated with Advanced Anti-DDoS, ECS, WAF, and database security services to display the security protection status in a centralized manner. HUAWEI CLOUD employs its situation awareness (SA) analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. The Big Data security analytics system incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks, including the most common cloud attacks such as brute force attacks, port scanning, zombie attacks, web attacks, unauthorized web access, and APT attacks. In addition, the system performs real-time evaluation of the security posture of HUAWEI CLOUD, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping HUAWEI CLOUD take necessary security precautions.

5.4 Response and recovery

5.4.1 Governance and preparation of incident response and recovery

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.1.1	Governance of incident response and recovery	Low: the customer shall establish a clear accountability assignment across the institution with regards to cyber incident response and recovery Medium: in addition to the above control, the customer shall develop an actionable plan to respond to and recover from a detected cyber event. High: in addition to the above control, the customer shall formulate an enterprise- wide plan to respond to and recover from a detected cyber event.	HUAWEI CLOUD has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. HUAWEI CLOUD has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, 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. In addition, HUAWEI CLOUD analyzes the root causes of security incidents and formulates preventive and preventive measures. HUAWEI CLOUD periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring. HUAWEI CLOUD complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system to standardize the business continuity

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.1.2	Incident response and recovery preparatio n	Low: the customer shall establish processes and capabilities to effectively respond to and restore critical functions, processes, systems and activities that may be impaired due to a cyber incident. Medium: in addition to the above control, the customer shall develop a plan to recover and maintain any capability or service that may be impaired due to a cyber incident. High: the customer shall prepare plans and financial capabilities to recover and maintain any capability or service that may be impaired due to a cyber incident in real time manner, with minimal loss to operations.	management framework, purpose and scope, management objectives, roles, and responsibilities. In addition, under the framework of the system, business impact analysis and risk assessment are performed regularly, key activities and dependencies are identified risk levels are evaluated, and countermeasures are formulated for identified threats that may cause cloud service resource interruption, and business continuity plans and disaster recovery plans are formulated. It will be tested regularly and the test results will be annotated and documented for continuous improvement of the plan. In addition, HUAWEI CLOUD can help customers develop and test business continuity plans based on their needs. HUAWEI CLOUD provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.

5.4.2 Analysis, mitigation, and restoration

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.2.1	Analysis	Low: the customer shall establish the process of cyber event analysis and classification. Medium: the customer should establish a process for analyzing and classifying cyber events based on internal knowledge and assets. High: in addition to the above control, the customer should establish enterprise-wide perspective on incident awareness and management leveraging automation, where possible.	**Managed Threat Detection (MTD)** of HUAWEI CLOUD continuously detects whether the IP or domain name of the visitor in the IAM log, DNS log, CTS log, OBS log and VPC log generated by the user's operation in HUAWEI CLOUD in the target area is subject to potential malicious activities and unauthorized behaviors. If any abnormality is found, a timely alarm will be given. This service integrates three capabilities of AI intelligent engine, Threat Intelligence and rule baseline to realize threat detection. It intelligently detects abnormal access behaviors implied in log data from multiple cloud services (including IAM service, DNS service, CTS service, OBS service and VPC service), proactively finds potential threats, generates alarm information for access behaviors that may have threats, and outputs alarm results. The user can check and process the alarm information through the alarm description, and timely deal with the potential threats before causing major losses such as information leakage, and upgrade and reinforce the service security, to protect the user's account security and ensure the stable operation of the service. **Situation Awareness (SA)** is a security management and situation analysis platform provided by HUAWEI CLOUD. It detects multiple cloud security risks, including DDoS attacks, brute force cracking, web attacks, backdoor Trojan horses, zombie hosts, abnormal behaviors, vulnerability attacks, and command and control. With big data analytics, SA can classify and analyze attack events, threat

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.2.2	Mitigation	Low: the customer shall develop a process to minimize the impact of cyber events, including cyber events occurred by a third party. Medium: in addition to the above control, the customer shall formulate a process for effective and prompt execution of the eradication plan, and formulate separate containment strategies for different types of major cyber-attacks; Develop a process for sharing cyber events and cyber best practices. High: in addition to the above controls, where applicable, the customer shall deploy automated mechanisms to support the incident management, containment, eradication and recovery processes to ensure that the staff responsible for incident management and the staff responsible for Network Threat Intelligence effectively cooperate during the incident.	alarms, and attack sources. This helps customers identify, collect, obtain evidence about information security events, and analyze events to reduce the possibility and impact of events in the future. In addition, SA can be associated with Advanced Anti-DDoS, ECS, WAF, and database security services to display the security protection status in a centralized manner. HUAWEI CLOUD formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, HUAWEI CLOUD can promptly notify financial institutions 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 financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation. HUAWEI CLOUD trains and tests information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training to ensure that critical incidents can be handled in a timely manner. In addition, security responders perform forensic analysis when a server/application is suspected to have been

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			compromised. HUAWEI CLOUD periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.
5.2.3	Restoration and quality assurance testing	Low: the customer shall establish and validate the effectiveness of processes in restoring the impacted functions, services, and data in a timely and secure manner. Medium: the customer shall establish and validate the effectiveness of processes in restoring the impacted functions, services, and data in a timely, secure, and resilient manner High: the customer shall establish and validate the effectiveness of processes in restoring the impacted functions, services, and data in a timely, secure, resilient, and cost optimized manner for the entire institution.	User data can be replicated and stored on multiple nodes in HUAWEI CLOUD 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. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of HUAWEI CLOUD services and safeguards customers' service and data security. 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.

5.4.3 Cyber forensics

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.3.5	Evidence retention and storage	Low: the customer should define the retention period of evidence. Medium: the customer should establish appropriate processes to store or archive evidence as required. High: N/A.	HUAWEI CLOUD uses a centralized log big data analysis system to collect management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. The logs are retained for more than 180 days. Security measures are taken during log storage to prevent logs from being tampered with to ensure that cyber security event backtracking and compliance are supported. To ensure log data security, security logs are backed up or archived in a unified manner. According to data security management requirements, security log application and permission are restricted. Only authorized personnel can query security logs for necessary reasons to ensure controlled use. In addition, **Cloud Trace Service (CTS)** records operations on cloud service resources for tenants. Many products and services also provide the log recording function. Tenants can select the log retention period based on their requirements to effectively support abnormal activity analysis. HUAWEI CLOUD formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, HUAWEI CLOUD can promptly notify financial

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			institutions 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 financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation. HUAWEI CLOUD trains and tests information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training to ensure that critical incidents can be handled in a timely manner. In addition, security responders perform forensic analysis when a server/application is suspected to have been compromised. HUAWEI CLOUD periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.

5.4.4 Communication and improvement

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.4.1	Escalation	Low: the customer should establish a process to inform the appropriate stakeholders of potential cyber events. Medium: in addition to the above controls, the communication procedures developed by the customer shall include procedures for notifying other organizations of events that may affect them or their customers and for notifying the media of relevant events. High: N/A.	HUAWEI CLOUD formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, HUAWEI CLOUD can promptly notify financial institutions 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 financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation. HUAWEI CLOUD trains and tests information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training to ensure that critical incidents can be handled in a timely manner. In addition, security responders perform forensic analysis when a server/application is suspected to have been compromised. HUAWEI CLOUD periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.
5.4.2	Incident reporting	Low: the customer should establish a formal process to provide regular event reports to necessary stakeholders. Medium: the customer develops metrics and information dashboards for cyber events as part of the report. High: the customer should introduce automation to facilitate quicker escalation, reporting and response time.	

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
5.4.3	Improvement	Low: the customer should establish a formal improvement process to identify opportunities to improve response and recovery from past cyber events. Medium: in addition to the above control, the customer shall conduct simulation test exercises to evaluate the event response and recovery capability. High: in addition to the above control, the customer should regularly refer to all security incidents to conduct trend analysis and improve cybersecurity measures and policies.	

5.5 Situational awareness

5.5.1 Threat intelligence

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
6.1.1	Threat intelligence	Low: the customer should subscribe and use threat intelligence to monitor relevant cyber threats and strengthen their cyber risk management and control. Medium: in addition to the above control, the customer shall implement a formal cyber threat intelligence programme, regularly evaluate the applicability of cyber intelligence, implement protocols to collect information from the industry and the government, and maintain a centralized read-only repository of cyber threat intelligence. High: in addition to the above control, the customer shall establish a cyber intelligence framework, implement a formal threat intelligence programme, to automatically retrieve threat intelligence from multiple sources in real time, implement a threat analysis system, alert the threat and take necessary actions.	As a cloud service provider, in order to cooperate with customers to meet regulatory requirements: **Managed Threat Detection (MTD)** of HUAWEI CLOUD continuously detects whether the IP or domain name of the visitor in the IAM log, DNS log, CTS log, OBS log and VPC log generated by the user's operation in HUAWEI CLOUD in the target area is subject to potential malicious activities and unauthorized behaviors. If any abnormality is found, a timely alarm will be given. This service integrates three capabilities of AI intelligent engine, Threat Intelligence and rule baseline to realize threat detection. It intelligently detects abnormal access behaviors implied in log data from multiple cloud services (including IAM service, DNS service, CTS service, OBS service and VPC service), proactively finds potential threats, generates alarm information for access behaviors that may have threats, and outputs alarm results. The user can check and process the alarm information through the alarm description, and timely deal with the potential threats before causing major losses such as information leakage, and upgrade and reinforce the service security, to protect the user's account security and ensure the stable operation of the service. **Situation Awareness (SA)** is a security management and situation analysis platform provided by HUAWEI CLOUD. It detects multiple cloud security risks, including DDoS attacks, brute force cracking, web attacks, backdoor Trojan horses, zombie hosts, abnormal behaviors, vulnerability attacks, and command

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			and control. With big data analytics, SA can classify and analyze attack events, threat alarms, and attack sources. This helps customers identify, collect, and obtain evidence about information security events, and analyze events to reduce the possibility and impact of events in the future. In addition, SA can be associated with Advanced Anti-DDoS, ECS, WAF, and database security services to display the security protection status in a centralized manner. HUAWEI CLOUD employs its situation awareness (SA) analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. The Big Data security analytics system incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks, including the most common cloud attacks such as brute force attacks, port scanning, zombie attacks, web attacks, unauthorized web access, and APT attacks. In addition, the system performs real-time evaluation of the security posture of HUAWEI CLOUD, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping HUAWEI CLOUD take necessary security precautions.

5.6 Third-party risk management

5.6.1 External connections

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
7.1.1	Identify	Low: the customer create network and system data flow diagrams that identify all external connections and third parties connected to the network, and regularly review and update them. Medium: in addition to the above controls, the customer should identify and assess the risks associated with external connections. High: in addition to the above control, the customer shall implement appropriate risk mitigation strategies for the identified risks.	HUAWEI CLOUD data center has many nodes and complex functional areas. To simplify network security design, prevent the spread of cyber-attacks on HUAWEI CLOUD, and minimize the impact of attacks, HUAWEI CLOUD divides and isolates security zones, services based on ITUE.408 security zone division principles, and best cybersecurity practices in the industry. Nodes in a security zone have the same security level. HUAWEI CLOUD network architecture design, device selection, configuration, and O&M are considered. HUAWEI CLOUD uses multiple layers of security isolation, access control, and border protection technologies for physical and virtual networks, and strictly implements management and control measures to ensure HUAWEI CLOUD security. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and cybersecurity risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD maintains the latest network topology. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, public service, POD-Point of Delivery, OBS-Object-Based Storage, and OM-Operations Management. In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
7.1.2	Protect	Low: the customer shall connect the external network or information system through the management interface composed of the boundary protection equipment of the enterprise-wide security architecture. Medium: in addition to the above control, the customer shall implement control to limit unnecessary external network connection with the information system, grant access rights according to the need and the principle of least privilege, set default rejection of network communications traffic, and regularly monitor and test external third-party connections. High: in addition to the above control, the outbound traffic shall be routed through the predefined network choke-points, the inbound traffic shall be protected by network security devices, the centralized console or interface shall be used to monitor and manage the proxy server, and the boundary protection mechanism shall be adopted.	to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. HUAWEI CLOUD isolates data on the cloud by using the **Virtual Private Cloud (VPC)**. VPC uses the network isolation technology to isolate tenants at Layer 3 networks. Tenants can completely control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using **Virtual Private Network (VPN)** or **Direct Connect (DC)**, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configurate security and access rules on demand to meet tenants' fine-grained network isolation requirements. In terms of network border protection, HUAWEI CLOUD has established a solid and complete border and multi-layer security protection system, and deployed Anti-DDoS, IDS/IPS, and WAF protection mechanisms. Anti-DDoS quickly detects and defends against DDoS attacks and comprehensively defends against traffic attacks and application layer attacks in real time. WAF detects and defends against web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately. The IDS/IPS detects and blocks cyber-attacks from the Internet in real time and monitors abnormal host behaviors. HUAWEI CLOUD services support their published APIs for

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			configuration management and integration with enterprise customers' IT management and audit systems. Considering the important functions that APIs support in cloud services and security threats that APIs face at the HTTP application layer, the industry generally regards APIs as crucial security perimeters of cloud services and employs multi-layered protection mechanisms and measures to safeguard API security. APIs of HUAWEI CLOUD can be invoked through the API Gateway developed by Huawei, which supports the following API protection mechanisms and scenarios: (1) Identity authentication and authorization: HUAWEI CLOUD performs identity authentication on each API request through HUAWEI CLOUD IAM integration. Only users who pass identity authentication are allowed to access and manage cloud-monitoring information. The data transmission channel is encrypted using TLS. (2) Transmission protection: API calls must use TLS-based encryption to ensure the confidentiality of data during transit. As of this writing, all public APIs supported by the API gateway use TLS 1.2 for encryption and support Perfect Forward Secrecy (PFS) security feature. (3) Perimeter protection: Coupled with multi-layered advanced perimeter protection mechanism including anti-DDoS, IPS and WAF, the API Gateway can effectively protect against various threats and attacks. By offloading, the decryption of TLS encrypted traffic to the load balancer, the multi-layered advanced perimeter security mechanism is able to

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
			monitor plaintext traffic inbound or outbound through the API Gateway and block attacks as needed. (4) API traffic flow control: The API Gateway controls the frequency of each user's API access in order to ensure the availability and continuity of API-based access. The API Gateway supports the configuration of requests per second for flow control on a per-API and per-tenant basis. Flow control information must be configuration on the API gateway for each public API. The API Gateway achieves separate flow control for each setting according to the maximum API access count by all HUAWEI CLOUD tenants within one-time measurement unit and the maximum API access count by each HUAWEI CLOUD tenant within one-time measurement unit.

5.6.2 Third-party management

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
7.2.1	Contract management	Low: the customer shall sign a contract with a third party connected to the network and handling sensitive or critical institutional data on relevant security and privacy requirements, specifying the security and privacy responsibilities of the third party, the claim rights of the institution against the breach of the third party, and the data return or destruction requirements upon the termination of the contract. Medium: in addition to the above control, the customer shall specify the responsibility for the notification of cybersecurity events and vulnerability in the agreement with the third party. High: in addition to the above control, the customer shall establish a termination/exit strategy with a third party, conduct regular tests, and submit high- and medium-risk items and their treatment methods to the management for endorsement.	HUAWEI CLOUD clearly defines the security responsibility-sharing model with customers. For details of the responsibility-sharing model, please refer to Chapter 3 of this article. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of customer. HUAWEI CLOUD may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
7.2.2	Due diligence	Low: the customer shall conduct full due diligence on the cybersecurity capability and personnel competency of the third-party service provider. Medium: the customer shall regularly conduct security assessment or audit on the third-party service provider. High: in addition to the above control, the customer shall develop and implement procedures for regular security assessment of the cybersecurity posture of the subcontractor.	HUAWEI CLOUD will comply with the requirements specified in the agreement signed with the customer, and assign dedicated personnel to actively cooperate with the customer in monitoring and risk assessment on HUAWEI CLOUD. 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.

5.6.3 Ongoing monitoring of third-party risk

No.	Control Principle	Customer Responsibility	HUAWEI CLOUD Response
7.3.1	Ongoing monitoring of third-party risk	Low: the customer should establish regular cybersecurity monitoring procedures for third parties that are connected to the network and handle sensitive or critical data of the organization. Medium: in addition to the above control, the customer shall consider the adjustment of the depth and frequency of the third-party monitoring based on the risk of the third party. High: in addition to the above control, the customer shall conduct Periodic on-site assessment or review of the third party's security auditor report, and track the access of the third party's employees to sensitive and critical data on the institutional hosted system based on the principle of least privilege.	HUAWEI CLOUD will comply with the requirements specified in the agreement signed with the customer, and assign dedicated personnel to actively cooperate with the customer in monitoring and risk assessment on HUAWEI CLOUD. HUAWEI CLOUD has obtained ISO 27001; ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications HUAWEI CLOUD has obtained many authoritative security and privacy protection certificate in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on HUAWEI CLOUD. Requirements for obtaining third-party audit reports can be specified in the agreement signed by the customer based on the actual situation. HUAWEI CLOUD has established a comprehensive supplier management mechanism. It strictly manages the security of outsourcers and outsourced personnel, and regularly audits and evaluates suppliers' security. HUAWEI CLOUD transfers customers' security requirements in contracts to suppliers to ensure that the products and services provided by suppliers can meet the security requirements of HUAWEI CLOUD customers. In addition, HUAWEI CLOUD will notify customers in a timely manner when important suppliers change based on customer requirements.

6 Conclusion

This whitepaper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the C-RAF 2.0 maturity assessment matrix and shows that HUAWEI CLOUD complies with key regulatory requirements issued by Hong Kong Monetary Authority of China (HKMA). This aims to help customers learn more about HUAWEI CLOUD's compliance status with Hong Kong SAR, China's regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this Whitepaper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of financial industry in Hong Kong SAR, China on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This whitepaper is for reference only and does not have any legal effect or constitute any legal advice. Customers should assess their own situation when using cloud services and be responsible for ensuring compliance with relevant financial industry regulatory requirements in Hong Kong SAR, China when using HUAWEI CLOUD.

7 Version History

Date	Version	Description
August 2022	1.0	First release