HUAWEI CLOUD User Guide to Financial Services Regulation & Guidelines in KSA

Issue 1.0

Date 2022-07-12

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud 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

In the recent ware of technological development, more and more financial institutions are seeking to transform their businesses. They want to leverage advanced technologies to improve continuous availability of services and effective protection of sensitive data. To standardize the use of information technology in the financial industry, the Saudi Arabian Monetary Authority (SAMA) has released regulatory requirement. These requirements address risk management, outsourcing management, and cloud computing implementation of FIs in the Kingdom of Saudi Arabian.

Huawei Cloud is committed to helping FIs meet the regulatory requirement and continuously providing FIs with cloud services and business operating environments that meet industrial standards. This document describes how Huawei Cloud will assist the Kingdom of Saudi Arabian FIs in meeting the regulatory requirements in the following guidelines and notices for cloud services.

1.2 Introduction of Applicable Saudi Arabia Financial Regulatory Requirements

Saudi Arabian Monetary Authority (SAMA): SAMA is the Central Bank of the Kingdom of Saudi Arabia whose functions include issuing currency, supervising commercial banks, managing foreign exchange reserves, promoting price and exchange rate stability, and ensuring the development and soundness of the financial system.

The SAMA issued the Cybersecurity Framework in May 2017 to enable financial institutions regulated by SAMA (“the financial institutions”) to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services.

1.3 Definition

- **Huawei Cloud**

  Huawei Cloud is Huawei's cloud service brand, dedicated to providing stable, reliable, secure, credible, sustainable and innovative cloud services.

- **Outsourcing**

  Means contracting with a service provider to perform operations that are usually done partly or completely by FIs themselves.

- **Customer**

  Registered users having a business relationship with Huawei Cloud.

- **Vendor**

  Entities and Branches of Entities that provide services to the financial institutions under outsourcing arrangements.

2 Huawei Cloud Security and Privacy Compliance

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 services and platforms have obtained the following certifications:

Certification	Description
ISO 20000:2011	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.
Classified Cybersecurity Protection of China's Ministry of Public Security	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.

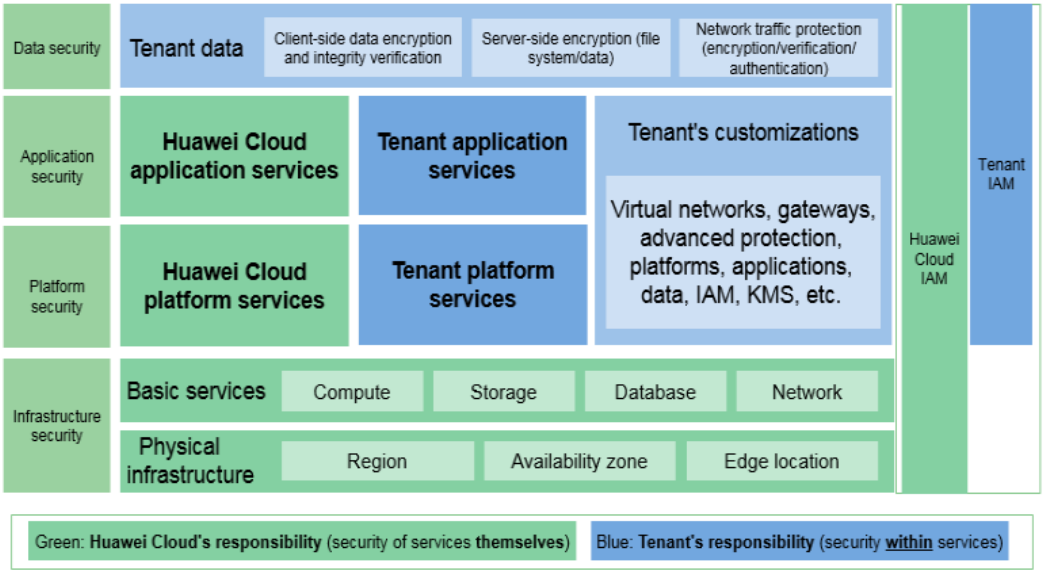
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that Huawei Cloud has achieved internationally recognized best practices in information security management.
Singapore MTCS Level 3 Certificatioin	The Multi-Tier Cloud 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).
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 CSPs can provide effective IT services to meet the requirements of customers and businesses.
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.
ISO 27018:2014	ISO 27018 is an international code of conduct that focuses on the protection of personal data in the cloud. The adoption of ISO 27018 indicates that Huawei Cloud has met the requirements of an internationally complete personal data protection and management system.
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.
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.

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.
TRUCS	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that Huawei Cloud complies with the most detailed standard for cloud service data and service assurance in China.
Gold O&M (TRUCS)	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	The certification is China's first cloud service user data security assessment mechanism after the Cyber Security Law takes effect. The first batch of Huawei Cloud passed this certification.
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT)	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 private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that Huawei Cloud complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification – Cyberspace Administration of China(CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. Huawei Cloud e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei eGovernment cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.

International Common Criteria EAL 3+Certification	Common Criteria (CC) certification is a highly recognized international standard for information technology products and system security. Huawei Cloud FusionSphere passed CC EAL 3+ certification, indicating that the Huawei Cloud software platform is highly recognized worldwide.

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 customers to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the customer and Huawei Cloud:



As shown in the above model, the privacy protection responsibilities are distributed between Huawei Cloud and customers as below:

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

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

For details on the security responsibilities of both Customers 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 the Requirements of SAMA Cybersecurity Framework

The SAMA Cybersecurity Framework defines principles and objectives for initiating, implementing, maintaining, monitoring and improving cyber security controls. It covers four domains: cybersecurity leadership and governance, cybersecurity risk management, cybersecurity operation and technology and third-party cybersecurity.

The following summarizes the control requirements associated with cloud service providers in the guide and details how Huawei Cloud can help meet these control requirements as a cloud service provider.

5.1 Cyber Security Leadership and Governance

SAMA Cyber Security Framework 3.1 “Cyber Security Leadership and Governance" requires financial institutions to establish appropriate cybersecurity management mechanisms, covering cybersecurity governance areas such as cybersecurity policies and procedures, awareness and training, roles and responsibilities. The relevant control requirements and practices of Huawei Cloud are as follows:

5.1.1 Cyber Security Policy

To document the financial institution's cybersecurity commitment and objectives of cyber security, and to communicate this to the relevant stakeholders.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibility

1	The cyber security policy should be defined, approved and communicated.	Huawei Cloud has established and implemented documented cybersecurity policies and procedures to provide guidance for operational cybersecurity management. Cybersecurity policies and procedures must be approved by managers before they are released, and employees can view the policies and procedures based on their authorization. Additionally, Huawei Cloud regularly conducts employee training every year in terms of company policies and culture.	The customer's cybersecurity department should develop cybersecurity policies and procedures, approved by the head of the organization or his/her delegate, and disseminated to relevant parties inside and outside the organization.
2	The cyber security policy should be reviewed periodically according to a predefined and structured review process.	Huawei Cloud reviews cybersecurity management policies and processes at least once a year and updates them as needed to reflect changes in business objectives or risk environments. Changes to policies and processes require senior management approval. In addition, Huawei Cloud has a dedicated audit team to regularly evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators, and report the survey results and suggestions to the top management.	Customers should periodically review and update cybersecurity policies and procedures based on planned frequency or changes in external regulation, and maintain a record of revisions.
3	The cyber security policy should be:		
b	Supported by detailed security standards (e.g., password standard, firewall standard) and procedures.	Huawei Cloud has established a comprehensive set of cyber security policies and procedures based on various international and industry standards, laws and regulations, regulatory requirements, and best practices in the industry, including but not limited to CIS, PCI DSS, NIST CSF, and CSA CCM.	Customer's cybersecurity policies and procedures can refer to industry technical security standards.

c	Based on best practices and (inter) national standards.	Huawei Cloud has established a comprehensive set of cyber security policies and procedures based on various international and industry standards, laws and regulations, regulatory requirements, and best practices in the industry, including but not limited to CIS, PCI DSS, NIST CSF, and CSA CCM.	Customer's cybersecurity policies and procedures can refer to industry technical security standards.
d	Communicated to relevant stakeholders.	Huawei Cloud ensures the implementation of the cyber security system in all systems, regions, and processes, and actively promotes communication with stakeholders, such as governments, customers, partners, and employees, to ensure that stakeholders can receive information about Huawei Cloud cyber security in a timely and effective manner.	Customer should actively communicate with the relevant stakeholders.
4	The cyber security policy should include:		
a	A definition of cyber security.	Huawei Cloud has formulated management requirements for cybersecurity and privacy protection, which clarifies that Huawei Cloud will build and fully implement an end-to-end cybersecurity system as an important strategy, comply with applicable laws and regulations of the business location, and fully meet customers' cybersecurity needs.	Customer's cyber security policy should include the definition of cyber security.
c	A statement of the board’s intent, supporting the cyber security objectives.	Huawei's leadership issued a statement on building a cybersecurity assurance system, which specified Huawei's cyber security strategy, committed Huawei's responsibility for network and obligation security assurance as an important attribute of the company, and established and improved a sustainable and reliable security assurance system. The strategy was approved by the company's top management.	Customer's board of directors should support cybersecurity objectives in a clear way.

d	A definition of general and specific responsibilities for cyber security.	From an organizational structure perspective, The Global Security and Privacy Committee (GSPC), being the highest cybersecurity management organization at Huawei, is responsible for company-level security policy decisions and the authorization of overall security strategies company-wide. GSPO is responsible for enact and implement Huawei end-to-end cybersecurity protection system. Huawei Cloud Computing Security & Privacy Office is responsible for formulating Huawei Cloud security policies, and periodically reviewing the implementation of the policies to ensure that the policies, specifications, and specific measures of security governance are implemented in the process of various business fields, and realize end-to-end security governance. Additionally, Huawei Cloud has clearly stipulated the cybersecurity responsibilities of all employees in the business team of each product and service. Huawei Cloud has set up roles specifically responsible for security and privacy protection to assume certain security management responsibilities. Cybersecurity-related roles and responsibilities are identified in writing and approved by the top management. Saudi Arabia Global Cyber Security & Privacy Officer follows Huawei's the highest cyber security strategies and implements them in Saudi Arabia.	Principal or representative of the customer's organization should define and approve the cybersecurity organizational structure and roles and responsibilities to ensure that there is no conflict of interest between the roles and responsibilities.

e	The reference to supporting cyber security standards and procedures.	Huawei Cloud complies with the security laws and regulations of the country or region where the CST is located and industry regulatory requirements, and refers to industry best practices to establish and manage a complete, reliable, and sustainable data security assurance system in terms of organization, process, specifications, technology, compliance, ecosystem, and other aspects.	Customers should refer to industry technical security standards to establish the cybersecurity policies and procedures.

f	Cyber security requirements that ensure: 1. Information is classified in a way that indicates its importance to the financial institution. 2. information is protected in terms of cyber security requirements, in line with the risk appetite. 3. owners are appointed for all information assets. 4. cyber security risk assessments are conducted for information assets. 5. relevant stakeholders are made aware of cyber security and their expected behavior (cyber security awareness program). 6. compliance with regulatory and contractual obligations are being met. 7. cyber security breaches and suspected cyber security weaknesses are reported. 8. cyber security is reflected in business	Huawei Cloud complies with the security laws and policies of all applicable countries and regions, international cyber security and cloud security standards, builds a comprehensive cyber security management system based on industry best practices, and formulates key areas and cyber security requirements for this area, including: 1/2/3. Huawei Cloud has formulated asset management procedures, which specify the classification and grading methods of information assets, and different protection measures based on the risk appetite of organizations. The authorization rules that should be followed for various types of assets, Huawei Cloud classifies information assets and uses dedicated tools to monitor and manage them. An asset list is generated and the asset owner is specified. 4. Huawei Cloud has established an information security risk management specification, which specifies the key processes that should be followed in risk management, the scope of risk management, the departments responsible for risk management, and the standards that should be followed in risk management. Determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. In addition, Huawei Cloud teams regularly perform information security risk assessments as required. 5. Huawei Cloud has established a series of cyber security training and learning mechanisms to ensure that employees' information security awareness	Customers should specify security requirements for asset management, cybersecurity risk assessment, cyber security awareness training, compliance, vulnerability management, and business continuity.

	continuity management.	meets Huawei requirements. Employees are required to continuously learn cyber security knowledge and understand related policies and regulations, understand what to do and what not to do, and promise to comply with requirements. 6. Huawei Cloud specifies the compliance process in its cybersecurity policies and regularly identifies and records compliance requirements. In addition, Huawei Cloud has set up dedicated posts to maintain active contact with external parties to track changes in laws and regulations. When identifying laws and regulations related to Huawei Cloud services, Huawei Cloud will adjust internal security requirements and security control levels in a timely manner to track compliance with laws and regulations. 7. Huawei Cloud has established a security vulnerability management process, which standardizes the closed-loop process of warning, assessment, and fixing of security vulnerabilities in Huawei Cloud systems. It also requires regular critical security patches to reduce vulnerability risks and specifies the requirements of vulnerabilities classification, responsibilities allocation, and vulnerability handling. Additionally, Huawei Cloud has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures. 1. 8. Huawei Cloud has obtained the certification of the ISO22301 business continuity management system standard. Huawei Cloud performs	

		business impact analysis and risk assessment annually to identify critical activities and dependencies, assess risk levels, and develop response strategies for identified threats that may cause cloud service resource disruption and establish a business continuity plan.	

5.1.2 Cyber Security Awareness

To create a cybersecurity risk-aware culture where the financial institution's staff, third parties and customers make effective risk-based decisions which protect the financial institution's information.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security awareness programs should be defined, approved and conducted to promote cyber security awareness and to create a positive cyber security culture.	According to the information security awareness training plan, Huawei Cloud continuously provides security awareness training for employees during their on-the-job period to raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations.	Customers should follow the established cybersecurity awareness training plan and train employees.

3	The cyber security awareness program should target cyber security behaviors by tailoring the program to address the different target groups through multiple channels.	Huawei Cloud has established a training mechanism to improve employees' awareness of information security and design appropriate training solutions for employees based on different roles and positions. An information security awareness training plan has been developed. The awareness education includes but is not limited to on-site lectures, online video courses, information security presentation, and case study.	Customers should develop a comprehensive security awareness and skill training management mechanism, develop training contents based on the functions and roles of the trainees, and regularly analyze and update the training contents.
4	The activities of the cyber security awareness program should be conducted periodically and throughout the year.	Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. The training frequency for general employees is at least once a year, and the training frequency for core employees is higher. New employees must pass information security and privacy protection training and exams before passing the probation. For On-duty employees, Huawei incorporates cyber security into the Employee Code of Conduct. Through the annual regular learning, examination, and performance appraisal measures, Huawei conducts performance appraisals for internal employees every six months to convey the company's requirements for all employees in the cyber security field and enhance employees' cyber security awareness.	Customers should conduct cyber security awareness training activities on a regular basis.

5	The cyber security awareness program should at a minimum include: a. an explanation of cyber security measures provided. b. the roles and responsibilities regarding cyber security. c. information on relevant emerging cyber security events and cyber threats (e.g., spear-phishing, whaling).	Huawei Cloud has established a series of cyber security training and learning mechanisms to ensure that employees' information security awareness meets Huawei requirements. Employees are required to continuously learn cyber security knowledge and understand related policies and regulations. It covers topics such as secure handling of phishing emails, secure handling of mobile devices and storage media, secure Internet browsing, and secure use of social media. Carry out various cyber security publicity activities for all employees, including cyber security community operation, publicity of typical cyber security cases, cyber security activity week, and cyber security animations, to raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations.	Customers should develop a cybersecurity awareness plan that covers the latest cyber threats and how to protect against them.
6	The cyber security awareness program should be evaluated to: a. measure the effectiveness of the awareness activities. b. formulate recommendations to improve the cyber security awareness program.	Huawei Cloud reviews and updates the personnel awareness training plan annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in processes of each business domain.	Customers should periodically review the implementation of the cybersecurity awareness program based on the program's frequency.

5.1.3 Cyber Security Training

To ensure that staff of the financial institutions are equipped with the skills and required knowledge to protect the financial institution’s information assets and to fulfil their cyber security responsibilities.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	Specialist or security-related skills training should be provided to staff in the financial institution’s relevant functional area categories in line with their job descriptions, including: a. key roles within the organization. b. staff of the cyber security function. c. staff involved in developing and (technically) maintaining information assets. d. staff involved in risk assessments.	Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. The training frequency for general employees is at least once a year, and the training frequency for core employees is higher. Huawei Cloud implements a specialized personnel management program for key positions such as development personnel, O&M engineers, and cybersecurity function personnel, including On-boarding security review, On-the-job security training and enablement, Onboarding qualifications management, Off-boarding security review. New employees must pass information security and privacy protection training and exams before passing the probation. On-duty employees need to select courses to study and take exams based on their business roles. Managements must attend information security training and workshops.	Customers should provide the necessary and customized mix of training and expertise to those directly involved in cybersecurity.

5.2 Cyber Security Risk Management and Compliance

SAMA Cyber Security Framework 3.2 "Cyber Security Risk Management and Compliance" requires financial institutions to manage cyber security risks in a systematic way, identify and manage cyber security risks from cyber security risk assessment to cyber security review and audit, and protect the organization's information assets in accordance with organizational policies, procedures, and relevant laws and regulations. The relevant control requirements and practices of Huawei Cloud are as follows:

5.2.1 Cyber Security Risk Management

To ensure cyber security risks are properly managed to protect the confidentiality, integrity and availability of the financial institution’s information assets, and to ensure the cyber security risk management process is aligned with the financial institution’s enterprise risk management process.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security risk management process should be defined, approved and implemented.	Huawei Cloud has established a cybersecurity risk management specification, which specifies the key processes that should be followed in risk management, the scope of risk management, the departments responsible for risk management, and the standards that should be followed in risk management, identify risks from multiple dimensions. Determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required.	Customers should establish cybersecurity risk management methods and procedures consistent with their organizational strategies.
2	The cyber security risk management process should focus on safeguarding the confidentiality, integrity and availability of information assets.	Huawei Cloud has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are require. Risk assessments covers various aspects of information security. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan.	Customers should implement the cybersecurity risk management procedures based on the confidentiality, integrity, and availability of assets.

4	The cyber security risk management process should be documented and address: a. risk identification. b. risk analysis. c. risk response. d. risk monitoring and review.	1. Risk management personnel identify inherent risks in each business area and assess risks based on threats and vulnerabilities faced by Huawei Cloud. Based on the inherent risk list, combined with the existing risk control measures, form the residual risk list and input the risks into the risk management platform in a timely manner, including the risk description, the area, the risk level, and the source of the risk 2. Based on business processes and asset management, Huawei Cloud security experts analyze and rate risks according to the probability and impact of identified risks. 3. Formally record the assessment and develop a risk treatment plan, and monitor the implementation of the risk treatment plan. 4. To ensure the effectiveness of risk control and continuous improvement, Huawei Cloud needs to regularly monitor risk metrics to control invalid risks, and incorporate them into risk management for continuous handling.	Customers should follow the cybersecurity risk management process and document risk identification, analysis, response, and monitoring and review.

5	The cyber security risk management process should address the financial institution's information assets, including (but not limited to): a. business processes. b. business applications. c. infrastructure components.	Huawei Cloud infrastructure components service teams regularly conduct cybersecurity risk assessments as required, and identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk treatment plan, and monitor the implementation of the risk treatment plan. Huawei Cloud will comply with the requirements specified in the agreement signed with the customer. Huawei Cloud will assign dedicated personnel to actively cooperate with the customer in monitoring and risk assessment on Huawei Cloud.	Customers should ensure manage the cybersecurity risk in business processes and business applications.
6	The cyber security risk management process should be initiated: a. at an early stage of the project. b. prior to critical change. c. when outsourcing is being considered. d. when launching new products and technologies.	Assess information security risks at the early stage of the project and periodically review information security impacts throughout the project delivery process. In addition, Huawei Cloud has formulated change management regulations and change processes. Changes must be reviewed in multiple phases to ensure that the operation and security of the organization are not adversely affected.	Customers should ensure that in the early stages of technology projects, before making major changes to technology infrastructure, during the planning phase of obtaining third party services and before going live for new technology services and products, the cybersecurity risk assessment procedures must be implemented, to ensure the continuous operation of organizational information security.

7	Existing information assets should be periodically subject to cyber security risk assessment based on their classification or risk profile.	The information security risk management regulations formulated by Huawei Cloud specify that the cyber security assessment scope includes the security risks of information assets. Based on the asset classification and potential defects or vulnerabilities, the cyber security risk assessment is performed periodically to identify risks that may be exploited by threats and cause asset damage.	Customers should periodically assess cyber security risks based on asset classification or risk status.

5.2.1.1 Cyber Security Risk Identification

To find, recognize and describe the financial institution’s cyber security risks.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	Cyber security risk identification should be performed.	Huawei Cloud has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are require.	Customers should identify potential cyber security risks.
2	Identified cyber security risks should be documented (in a central register).	Risk management personnel identify inherent risks in each business area and assess risks based on threats and vulnerabilities faced by Huawei Cloud. Based on the inherent risk list, combined with the existing risk control measures, form the residual risk list and input the risks into the risk management platform in a timely manner, including the risk description, the area, the risk level, and the source of the risk.	Customers should follow a cybersecurity risk assessment process to identify internal and external risks to the organization's assets, document the identified risks in a central register

3	Cyber security risk identification should address relevant information assets, threats, vulnerabilities and the key existing cyber security controls.	Risk management personnel identify risks involved in business scenarios, and conduct risk assessment based on threats and vulnerabilities faced by Huawei Cloud. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan.	Customers should identify cyber security risks for information assets, threats, vulnerabilities, and critical existing cyber security controls.

5.2.1.2 Cyber Security Risk Analysis

To analyze and determine the nature and the level of the identified cyber security risks.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	A cyber security risk analysis should be performed.	Huawei Cloud risk management personnel comply with cyber security risk management regulations. Based on business processes and asset management, Huawei Cloud security experts analyze and rate risks according to the probability and impact of identified risks, and formally record the assessment and develop a risk treatment plan.	Customers should perform cyber security risk analysis.
2	The cyber security risk analysis should address the level of potential business impact and likelihood of cyber security threat events materializing.	Huawei Cloud risk management personnel comply with cyber security risk management regulations. Based on business processes and asset management, Huawei Cloud security experts analyze and rate risks according to the probability and impact of identified risks, and formally record the assessment and develop a risk treatment plan.	Customers should analyze the cybersecurity risks to address the level of potential business impact and likelihood of cyber security threat events materializing.

5.2.1.3 Cyber Security Risk Response

To ensure cyber security risks are treated (i.e., accepted, avoided, transferred or mitigated).

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
2	Cyber security risk response should ensure that the list of risk treatment options are documented (i.e., accepting, avoiding, transferring or mitigating risks by applying cyber security controls).	Huawei Cloud risk management personnel comply with cyber security risk management regulations, assign risk ratings to threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan, which including rectification measures, plans, key milestones, and risk degradation standards, and control measures such as risk rectification, risk retention, risk avoidance, and risk transfer to reduce and eliminate risks to an acceptable range.	Customers should document the risk treatment options.
3	Accepting cyber security risks should include: a. the consideration of predefined limits for levels of cyber security risk. b. the approval and sign-off by the business owner, ensuring that: 1. the accepted cyber security risk is within the risk appetite and is reported to the cyber security committee. 2. the accepted cyber security risk does not contradict SAMA regulations.	Huawei Cloud follows the established cybersecurity risk management regulations. When the risk is accepted after the risk decision is made, the risk status will be maintained and no further control measures will be taken. When the business department reviews and chooses to accept the risk, it needs to be submitted to the risk administrator for a formal decision-making. The review and decision-making conclusions must be synchronized to the risk management platform. Huawei Cloud will not contradict the SAMA regulations when accepting cybersecurity risks.	Customers should ensure that the accepted cyber security risk is within the risk appetite and does not contradict SAMA.

4	Avoiding cyber security risks should involve a decision by a business owner to cancel or postpone a particular activity or project that introduces an unacceptable cyber security risk.	Huawei Cloud follows the established cybersecurity risk management regulations. When risks are too high or the cost of risk rectification measures is too high, and business benefits may exceed the impact of risks, Huawei Cloud takes measures to avoid risks.	Customers should specify the cybersecurity avoid measures, such as canceling or delaying specific activities or projects that cause cyber security risks.
5	Transferring or sharing the cyber security risks should: a. involve sharing the cyber security risks with relevant (internal or external) providers. b. be accepted by the receiving (internal or external) provider(s). c. eventually lead to the actual transferring or sharing of the cyber security risk.	Huawei Cloud follows the established cybersecurity risk management regulations. Huawei Cloud shares risks with external organizations. Risk sharing cannot completely eliminate risks, but can only reduce the economic loss caused by risks to a certain extent.	Customers should specify the cybersecurity transfer or share measures, such as sharing risks with internal or external parties.

6	Applying cyber security controls to mitigate cyber security risks should include: a. identifying appropriate cyber security controls. b. evaluating the strengths and weaknesses of the cyber security controls. 1. assessing the cost of implementing the cyber security controls. 2. assessing the feasibility of implementing the cyber security controls. 3. reviewing relevant compliance requirements for the cyber security controls. c. selecting cyber security controls. d. identifying, documenting and obtaining sign-off for any residual risk by the business owner.	Huawei Cloud follows the established cybersecurity risk management regulations, and reduces risks to an acceptable range by adding new control measures or adjusting existing control measures. Specifically, security control policies, processes, technical control measures, and compensation measures can be adopted, such as security monitoring, security audit, and emergency plan. After receiving the risk notification email, the risk contact person shall output the risk handling solution. The risk and process expert team shall review the advantages, disadvantages, feasibility, and compliance of the solution. Risk extension or risk acceptance must be decided by the relevant Huawei Cloud supervisor.	Customers should specify the cybersecurity mitigate measures and implement cyber security controls, and obtain sign-off for any residual risk by the business owner.

7	Cyber security risk treatment actions should be documented in a risk treatment plan.	Huawei Cloud follows the established cybersecurity risk management regulations. The risk contact person outputs a risk handling solution, including rectification measures, plans, key milestones, and risk degradation standards, and control measures such as risk rectification, risk retention, risk avoidance, and risk transfer to reduce and eliminate risks to an acceptable range.	Customers should record cyber security risk treatment actions should be documented in a risk treatment plan.

5.2.1.4 Cyber Risk Monitoring and Review

To ensure that cybersecurity risk treatment is carried out according to the treatment plan. To ensure that the revised or newly implemented cybersecurity controls are effective.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The cyber security treatment should be monitored, including: a. tracking progress in accordance to treatment plan; b. the selected and agreed cyber security controls are being implemented.	Huawei Cloud service teams regularly conducts cybersecurity risk assessments as required. Huawei Cloud identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk treatment plan, and monitor the implementation of the risk treatment plan. To ensure the effectiveness of risk control and continuous improvement, Huawei Cloud needs to regularly monitor risk metrics to control invalid risks, and incorporate them into risk management for continuous handling. Huawei Cloud needs to regularly monitor risk metrics to control invalid risks, and incorporate them into risk management for continuous handling. In addition, Huawei Cloud Computing Security & Privacy Office regularly organizes expert group meetings on cybersecurity assessments and major incident retrospectives, to identify relevant cybersecurity risks and conduct regular follow-up procedures for risk disposal. These reviews are used to ensure compliance with the company's risk management requirements.	Customers should define a cyber risk treatment and monitoring plan to dispose and monitor the identified risks.
2	The design and effectiveness of the revised or newly implemented cyber security controls should be reviewed.	Huawei Cloud Computing Security & Privacy Office regularly organizes expert group meetings on cybersecurity assessments and major incident retrospectives, to identify relevant cybersecurity risks and conduct regular follow-up procedures for risk disposal. Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review the design and effectiveness of security controls which are revised or newly implemented.

5.2.2 Regulatory Compliance

To comply with regulations affecting cyber security of the financial institution.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	A process should be established for ensuring compliance with relevant regulatory requirements affecting cyber security across the financial institution. The process of ensuring compliance should: a. be performed periodically or when new regulatory requirements become effective. b. involve representatives from key areas of the financial institution. c. result in the update of cyber security policy, standards and procedures to accommodate any necessary changes (if applicable).	Huawei Cloud specifies the compliance process in its cybersecurity policies and regularly identifies and records compliance requirements. In addition, Huawei Cloud has set up dedicated posts to maintain active contact with external parties to track changes in laws and regulations. When identifying laws and regulations related to Huawei Cloud services, Huawei Cloud will adjust internal security requirements and security control levels in a timely manner to track compliance with laws and regulations.	Customers should ensure that representatives from key areas of financial institutions regularly identify cyber security regulatory requirements and update cyber security policies based on the cyber security regulatory requirements or standards.

5.2.3 Cyber Security Review

To ascertain whether the cyber security controls are securely designed and implemented, and the effectiveness of these controls is being monitored.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	Cyber security reviews should be periodically performed for critical information assets.	Huawei Cloud has established a formal and regular audit plan, including continuous and independent internal and external assessments. The internal assessment continuously tracks the effectiveness of security control measures, and the external assessment audits as independent auditors to verify the effectiveness of the implementation and operation of the Huawei Cloud control environment. Audit results are reviewed by management and corrective actions are followed up. At the same time, Huawei Cloud has a dedicated audit team that regularly evaluates the compliance and effectiveness of strategies, procedures, supporting measures and indicators, and report the results and recommendations of the investigation to the top management.	Customers should audit critical systems at least once a year, retain and protect audit records, and report audit findings and recommendations to management to determine compliance and effectiveness of cybersecurity controls..

2	Customer and internet facing services should be subject to annual review and penetration tests.	Huawei Cloud has developed the internal audit management process to standardize the internal audit principles, audit management process, and audit frequency. A dedicated audit team performs an internal audit on Huawei Cloud every year to check the running status of the company's internal control system and evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators. 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.	Customers should conduct periodic annual reviews and penetration testing of customer and internet facing services
3	Details of cyber security review performed should be recorded, including the results of review, issues identified and recommended actions.	Huawei Cloud has developed an internal audit management process, which requires the audit team to record the cyber security audit process, including but not limited to the audit plan, reviewers, review basis, corrective measures, follow-up audit, and audit report.	Customers should ensure that details of cybersecurity reviews are documented, including findings, issues and recommendations.
4	The results of cyber security review should be reported to business owner.	Huawei Cloud will report the audit results and recommendations to the top management. Management review and follow up on rectification to ensure that the finding issues are resolved and closed.	Customers should submit the findings and recommendations to the business owner.

5	Cyber security review should be subject to follow-up reviews to check that: a. all identified issues have been addressed. b. critical risks have been treated effectively. c. all agreed actions are being managed on an ongoing basis.	Huawei Cloud Computing Security & Privacy Office regularly organizes expert group meetings on cybersecurity assessments and major incident retrospectives, to identify relevant cybersecurity risks and conduct regular follow-up procedures for risk disposal. Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should follow cybersecurity reviews and be subject to follow-up reviews to ensure that all issues and key risks have been addressed effectively.

5.2.4 Cyber Security Audits

To ascertain with reasonable assurance whether the cyber security controls are securely designed and implemented, and whether the effectiveness of these controls is being monitored.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	Cyber security audits should be performed independently and according to generally accepted auditing standards and SAMA cyber security framework.	Huawei Cloud regularly hires independent third parties to provide external audit and verification services. These evaluators perform regular security assessment and compliance audits or checks. (E.g. SOC, ISO standards, PCIDSS audit) to assess the security, integrity, confidentiality, and availability of information and resources for an independent assessment of risk management content/processes. Huawei Cloud will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer.	Customers should perform independent cybersecurity audits to determine compliance with generally accepted auditing standards and the SAMA Cybersecurity Framework.

2	Cyber security audits should be performed according to the financial institution's audit manual and audit plan.	Huawei Cloud has established a formal and regular audit plan, including continuous and independent internal and external assessments. The internal assessment continuously tracks the effectiveness of security control measures, and the external assessment audits as independent auditors to verify the effectiveness of the implementation and operation of the Huawei Cloud control environment. Huawei Cloud will comply with the requirements specified in the agreement signed with the customer. Huawei Cloud will assign dedicated personnel to actively cooperate with the customer in monitoring and risk assessment on Huawei Cloud.	Customers should perform cybersecurity audits according to the organization's audit manual and audit plan.

5.3 Cyber Security Operations and Technology

"SAMA Cyber Security Framework" 3.3 "Cybersecurity Operations and Technology" requires financial institutions to develop policies and procedures for cybersecurity operations and security management, including asset management, identity and access management, application security, cryptography management, backup and recovery, cybersecurity incident management, etc. The relevant control requirements and practices of Huawei Cloud are as follows:

5.3.1 Human Resources

To ensure that financial institution staff's cyber security responsibilities are embedded in staff agreements and staff are being screened before and during their employment lifecycle.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The human resources process should define, approve and implement cyber security requirements.	Huawei Cloud has established personnel information security management regulations, which specify hierarchical information security management requirements, standardize the management of recruitment, training, audit, reward and punishment for internal and external employees, and specify the cyber security responsibilities.	Customers should develop and implement cybersecurity requirements for employees before, during, and after employment.
2	The effectiveness of the human resources process should be monitored, measured and periodically evaluated.	Huawei Cloud reviews and updates the established personnel information security regulations and procedures annually. In addition, the Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update personnel cybersecurity requirements on a regular basis as scheduled.
3	The human resource process should include:		
a	cyber security responsibilities and non-disclosure clauses within staff agreements (during and after the employment).	The employment agreement signed between the employee and the company contains confidentiality clauses, which clearly state the employee's cybersecurity responsibilities to ensure that the confidentiality clauses to be followed are confirmed before onboarding. Huawei Cloud employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities.	Customers should include cybersecurity requirements that personnel must comply with in the employment contract and confidentiality clauses.

b	staff should receive cyber security awareness at the start and during their employment.	Huawei Cloud has established a series of information security training and learning mechanisms to ensure that employees' information security awareness meets Huawei requirements. New employees must pass information security and privacy protection training and exams before passing the probation. Organize information security awareness training and information security knowledge publicity for On-duty employee annually.	Customers should regularly provide cybersecurity training for active employees.
c	when disciplinary actions will be applicable.	HUAWEI has established a strict security responsibility system and implemented an accountability mechanism for violations. Huawei Cloud holds employees accountable on the basis of behavior and results. According to the nature of Huawei Cloud employees' security violations and the consequences, the accountability handling levels are determined and handled in different ways. Those who violate laws and regulations shall be transferred to judicial organs for handling. Direct managers and indirect managers shall assume management responsibilities if they have poor management or knowingly inaction. The handling of violations will be aggravated or mitigated according to the attitude of the individual who violated the regulations and the cooperation in the investigation. Huawei Cloud's violation management policies are published internally for all employees to view and learn. And Huawei Cloud regularly organizes training to improve employees' understanding of violations, consequences of violations, and punitive measures.	Customers should take disciplinary action against personnel who do not meet the organization's cyber security requirements.

d	screening and background check.	Before appointment, Huawei Cloud conducts background checks on new employees who meet specific conditions through the established background check mechanism. In addition, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed.	Customers should screen and vet all candidates by conducting background checks prior to employment.
e	post-employment cyber security activities, such as: 1. revoking access rights. 2. returning information assets assigned (e.g., access badge, tokens, mobile devices, all electronic and physical information)	1. After the status changes, such as resignation or position change, employees and other third parties shall conduct a security review according to the transfer and resignation security review checklist, which includes the clearance or modification of the resignation account permissions. 2. When the contract/business relationship with the partner is terminated, the information generated in the cooperation project in the self-contained device should be deleted according to the cooperation agreement, and the assets provided by Huawei Cloud will be returned. Huawei Cloud has established an electronic flow of assets transfer when personnel resign/termination of cooperation, and implement assets transfer in accordance with the electronic process. Huawei Cloud employees must sign the resignation confidentiality commitment letter to confirm their ongoing information security responsibilities.	Customers should ensure that employees' permissions and assets are reviewed and recovered after they resign.

5.3.2 Physical Security

To prevent unauthorized physical access to the financial institution information assets and to ensure its protection.

No.	Specific control requirements	Huawei Cloud Response
1	The physical security process should be defined, approved and implemented.	Huawei Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures. The Huawei Cloud information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented.
2	The effectiveness of the physical security process should be monitored, measured and periodically evaluated.	Huawei Cloud review and update the established physical and environmental security procedures every year. At the same time, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of the policy to ensure that the policies, standards, specifications, and specific measures of security governance are implemented in various business areas.
3	The physical security process should include (but not limited to):	
a	physical entry controls (including visitor security);	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.
b	monitoring and surveillance (e.g., CCTV, ATMs GPS tracking, sensitivity sensors);	The Huawei Cloud information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, video surveillance, etc.) and different requirements for equipment access control (including photography equipment, storage media, etc.). At the same time, the data transfer policies and access control policies between zones have been formulated and implemented.

c	protection of data centers and data rooms;	Huawei Cloud has formulated regulations on confidential devices and media management, which specify requirements for device placement, protection, and access and formulate operation processes. Important components of the data center are stored in a dedicated electronic encryption safe in the warehousing system, and the safe is switched on and off by a dedicated person. Any spare components of the data center must be obtained by providing an authorized service ticket and must be registered in the warehousing management system. All physical access equipment and warehousing system materials are regularly counted and tracked by dedicated personnel. The equipment room administrator not only conducts routine security checks, but also audits data center access records irregularly to ensure that unauthorized personnel cannot access the data center.

d	environmental protection;	Huawei Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The Huawei Cloud O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of Huawei Cloud data centers. • **Electrical safety**: Huawei Cloud data centers employ a multi-level safety assurance solution to ensure 24/7 service availability and continuity. Daily electricity consumption at data centers relies on dual power supply from different power substations. Data centers are equipped with diesel generators, which are run in the event of power outage, and also Uninterruptible Power Supply (UPS), which provides temporary power as a backup. Data center power lines have voltage regulator and overvoltage protection. Power supply equipment is configured with redundancy and power lines run in parallel to ensure power supply to data center computer systems. • **Temperature and humidity control**: Huawei Cloud data centers are fitted with high precision air conditioning and automatic adjustment of centralized humidifiers to ensure that computer systems operate optimally within their specified ranges of temperature and humidity. Hot and cold air channels for computer cabinets are properly designed and positioned. Cold air channels are sealed to prevent isolated hot spots. The space beneath the raised floor is used as a static pressure box to supply air to computer cabinets. • **Fire control**: Huawei Cloud data centers comply with Level-1 design and use Class-A fireproof materials for their construction in compliance with country-specific fire control regulations. Flame retardant and fire-resistant cables are used in pipelines and troughs, alongside power leakage detection devices. Automatic fire alarm and fire

		extinguishing system is deployed to quickly and accurately detect and report fires. Automatic alarm system links with power supply, monitoring, and ventilation systems such that the fire extinguishing system can activate itself even when unattended, autonomously keeping fires under control. • **Routine monitoring**: Huawei Cloud personnel conduct daily patrols and routine inspections of power, temperature, humidity, and fire controls in all data centers, which allows for the timely discovery of safety hazards and ensures smooth operation of all data center equipment. • **Water supply and drainage**: The water supply and drainage system at each Huawei Cloud data center is designed, implemented, and operated to an exacting standard, ensuring that main valves function as per specification and key personnel are aware of valve locations. This prevents water damage to the data center equipment, especially computer information systems. Data center buildings reside on elevated ground with peripheral green drains and each floor is raised, which speeds up water drainage and reduces the risk of flooding. Data center buildings all meet Level-1 water resistance requirements, ensuring that rainwater does not seep through roofs and walls into the data center, and that there is proper drainage in case of a flood. • **Anti-static control**: Huawei Cloud data centers are paved with anti-static flooring materials and have wires connect raised floor brackets to grounding networks, discharging static electricity from computer equipment. Data center roofs are fitted with lightning belts, and power lines are fitted with multiple-level lighting arresters, diverting the current safely to grounding networks.

e	protection of information assets during lifecycle (including transport and secure disposal, avoiding unauthorized access and (un)intended data leakage.	As the cloud service provider of the financial institutions, Huawei Cloud has formulated and implemented regulations on mobile media management, which specify: ● Huawei Cloud requires that storage media containing Huawei confidential information must be marked. Confidential data shall be marked or labeled according to the data security level, and the security level shall be stated. Labels must be attached to the exterior of media in transit or facilities authorized to store the media, and to the exterior of locked containers used for transporter media. ● Huawei Cloud requires storage media to be stored in a controlled access area or in a locked cabinet. When a storage media enters or exits a controlled area, the detailed information from outbound to inbound must be reconciled and tracked in a closed-loop manner. ● Ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media. ● All types of mobile media shall be managed by dedicated personnel. Approval is required for borrowing and must be formatted after use. The media are cleared and scrapped according to the classification. Huawei Cloud achieves data cleaning, disk demagnetization through a variety of ways, and records the destruction operation. Dedicated personnel manage devices that contain storage media on Huawei Cloud. After the devices are used, dedicated personnel format the devices. When a storage media that stores HUAWEI's confidential information is scrapped, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting.

5.3.3 Asset Management

To support the financial institution in having an accurate and up-to-date inventory and central insight in the physical / logical location and relevant details of all available information assets, in order to support its processes, such as financial, procurement, IT and cyber security processes.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The asset management process should be defined, approved and implemented.	Huawei Cloud has formulated asset management procedures, which specify the classification and grading methods of information assets and the authorization rules that should be followed for various types of assets. In addition, Huawei Cloud has established information asset confidentiality management requirements, which specify the confidentiality measures that Huawei Cloud should take for information assets at different levels, and standardize the use of assets to ensure that the company's assets are properly protected and shared.	Customers should establish formal asset management procedures, classify their assets and define their owners.
2	The effectiveness of the asset management process should be monitored, measured and periodically evaluated.	Huawei Cloud reviews and updates the asset management regulations and procedures annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should periodically review and update cybersecurity requirements for information and technology assets as scheduled.
3	The asset management process should include:		

a. b.	a unified register. ownership and custodianship of information assets.	Huawei Cloud regularly identifies hardware, software, data, personnel, and services. Huawei Cloud uses the Cloud Asset Management system to monitor the inventory and maintenance status of Huawei Cloud information assets recorded on the asset management platform in real time, classify, monitor, and manage information assets, and generate an asset list for each asset. In addition, In Huawei Cloud, configuration managers are assigned to manage the configuration of all services, the resource configuration model consists of hosts, service trees, cloud infrastructures, and network devices. Configuration item mapping and resource lifecycle management are constructed to ensure stable and secure O&M in production environment. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes. Huawei Cloud uses IPAM to centrally manage IP resources. In addition, the HSP host security platform suite is deployed on the Huawei Cloud platform to provide network security protection for platform assets.	Customers should create a unified register list and define ownership and custodianship of information assets. 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.

c	the reference to relevant other processes, depending on asset management.	Huawei Cloud complies with other security regulations defined by Huawei Cloud during asset management. According to the importance and impact of assets on services to classify assets by referring the security policy. Conduct risk assessment on assets of different levels by referring to cyber security risk management regulations, identify risks of asset damage caused by potential defects or vulnerabilities of assets being exploited by threats, and comply with roles and responsibilities in media management regulations, data management regulations, and security incidents management regulations to protect the lifecycle of assets.	Customers should refer to relevant processes when developing the asset management procedures.

d	information asset classification, labeling and handling.	Huawei Cloud uses the Cloud Asset Management (CAM) system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and create an asset list for each asset. In addition, In Huawei Cloud, configuration managers are assigned to manage the configuration of all services, the resource configuration model consists of hosts, service trees, cloud infrastructures, and network devices. Configuration item mapping and resource lifecycle management are constructed to ensure stable and secure O&M in production environment. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes. Huawei Cloud has implemented hierarchical data management and graded data based on confidentiality integrity, availability, and compliance. Data is classified into multiple security levels and defined separately. It also specified security implementation requirements, audit requirements, emergency response, and drill requirements for different levels of data. Each business domain marks the security level of the data in its domain according to the data grading standards.	Customers should mark the asset classification based on legal provision, asset value, and asset importance and sensitivity to the organization.

e	the discovery of new information assets.	Huawei Cloud uses the Cloud Asset Management (CAM) system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and create an asset list for each asset. In addition, Huawei Cloud uses an automated tool to collect basic configuration information about physical machines, VMs, containers, and network devices, such as specifications and OS configurations. This tool interconnects with CMDB to report the configuration information to CMDB, ensuring data accuracy.	Customers should discover new information assets in a timely manner and maintain the latest asset list.

5.3.4 Cyber Security Architecture

To support the financial institution in achieving a strategic, consistent, cost effective and end-to-end cyber security architecture.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security architecture should be defined, approved and implemented.	Huawei Cloud follows the cybersecurity management regulations established by Huawei, which specify relevant control requirements such as network isolation, network access security and cybersecurity defense, so as to ensure that organizations are protected from cybersecurity risks caused by malicious network intrusion.	Customers should establish formal systems and network management procedures to ensure that the organization's network is protected from security risks.

2	The compliance with the cyber security architecture should be monitored.	Huawei Cloud reviews and updates the established network management regulations and procedures annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should periodically review and update the security requirements in cybersecurity management as scheduled.
3	The cyber security architecture should include:		

a	a strategic outline of cyber security capabilities and controls based on the business requirements.	Huawei Cloud follows the cybersecurity management regulations and implements a formal environmental isolation mechanism. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks. In addition, Huawei Cloud provides multi-layer protection measures. For example, access control and border protection technologies are used to implement coordinated protection against external attacks and strictly implement corresponding management and control measures to ensure Huawei Cloud security. Based on business functions and network security risks, the Huawei Cloud data center network is mapped into different security zones to achieve network isolation using both physical and logical controls to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats	Customer should establish a cybersecurity capabilities and controls based on the business requirements.

b	approval of the defined cyber security architecture.	Huawei Cloud maintains the latest network topology. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration as well as O&M, and network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks. In addition, Huawei Cloud strictly implement corresponding management and control measures to ensure Huawei Cloud security.	Customers should record the actual state of the network topology.
c	the requirement of having qualified cyber security architects.	Huawei's technical security personnel consists of some of the world's leading experts and specialists in information security, product security, application security, system security, network security, cloud service security, O&M security, and privacy protection.	Customers should have qualified cyber security architects.
d	design principles for developing cyber security controls and applying cyber security requirements (i.e., the security-by-design principle).	In the design phase, Huawei Cloud considers the capability of the solution in border protection from the functional architecture to effectively deal with common border risks. Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the industry best practices on network security. Nodes in the same security zone are at the same security level. In addition, Huawei Cloud standardizes the deployment and release processes of products/ services that use the DevOps development mode, which regulates the requirements for environment isolation, to improve the stability of the production environment.	Customer should consider the security principles in the design when developing and applying network security control requirements.

e	periodic review of the cyber security architecture.	Huawei Cloud maintains the latest network topology. Huawei Cloud reviews and updates the established network management regulations and procedures annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should periodic review of the cyber security architecture.

5.3.5 Identity and Access Management

To ensure that the financial institution only provides authorized and sufficient access privileges to approved users.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The identity and access management policy, including the responsibilities and accountabilities, should be defined, approved and implemented.	Huawei Cloud has formulated requirements on user account permission management, which standardizes the process for employees to follow when applying for, maintaining, and deregistering permissions. In addition, Huawei Cloud has formulated account permission management requirements and processes for Huawei Cloud platform accounts, specifying account classification management and access control policies.	Customers should establish an identity authentication and access control management mechanism to restrict and monitor access to the system.

2	The compliance with the identity and access policy should be monitored.	Huawei Cloud reviews and updates the established identity and access management regulations and procedures every year. In addition, the Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in processes of each business domain.	Customers should regulars review and update the cybersecurity requirements for identity and access management periodically based on the planned frequency.
3	The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established identity and access management regulations and procedures every year. In addition, the Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in processes of each business domain.	Customers should regulars review and update the cybersecurity requirements for identity and access management periodically based on the planned frequency.
4	The identity and access management policy should include:		

a	business requirements for access control (i.e., need-to-have and need-to-know)	Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimized permission assignment and strict behavior audit ensure that unauthorized access is not performed.	Customers should implement role-based access control and permission management, complying with the minimum principle of on-demand knowledge and use. Customers can use Huawei Cloud Identity and Access Management (IAM) to grant hierarchical and fine-grained authorization. Administrators can plan the permissions to use cloud resources based on users' responsibilities. In addition, administrators can set security policies for users to access cloud service systems, such as ACLs, to prevent malicious access from untrusted networks.
b	user access management (e.g., joiners, movers, leavers):		
1	all identified user types should be covered (i.e., internal staff, third parties).	Huawei Cloud has formulated requirements on user account permission management, which standardize the account application process for different user types, such as internal employees and external third-party employees.	Customers should ensure all identified user types should be covered.

2	changes of job status or job positions for internal staff (e.g. joiner, mover and leaver) should be instigated by the human resources department.	Huawei Cloud employees use a unique identity in the internal office network, and have established comprehensive account lifecycle management regulations and processes. A new employee must be approved and authorized by the president of the employing department and the department's HR. The management platform will create an account for the employee after approval, and the account is used for the employee to log in to various systems or platforms within Huawei Cloud. When a Huawei Cloud employee is transferred to another position, the transfer personnel must apply for the transfer and the e-flow will be automatically transferred to the department director where the employee belongs. The department director confirms with the system administrator and HR that the employee's current permissions have been canceled and confirms the employee's transfer in the e-flow. Before the employee's resignation e-flow completes, the e-flow must be reviewed by the department director and HR to ensure that the employee's permissions have been canceled and the employee's account will be automatically deregistered after the employee resigns.	Customers should ensure that the changes of job status or job positions for internal staff should be instigated by the human resources department.

3	changes for external staff or third parties should be instigated by the appointed accountable party.	The management owner submits an account/right application e-flow for the outsourced personnel and obtains the approval and authorization from the related director. After the authorization is complete, the internal system automatically creates an internal account with only basic rights for the outsourced personnel and grants only the minimum resource access rights required to complete the work. The management owner submits a deregistration application when the outsourced personnel leaves the site or no longer needs the account or permission.	Customers should ensure that the changes for external staff or third parties should be instigated by the appointed accountable party.

4	user access requests are formally approved in accordance with business and compliance requirements (i.e., need-to-have and need-to-know to avoid unauthorized access and (un)intended data leakage))	Huawei Cloud employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. Identity and Access Management (IAM) is used to control and manage user access to cloud services. All O&M, device, and application accounts are centrally managed. All accounts are centrally monitored and automatically audited through the unified audit platform. Therefore, the entire account lifecycle is well managed, from account creation, permissions granting, permissions verification and access granting, and account and permissions deletion. If the account user wants to use the account, the account administrator can start the authorization process and authorize the account by means of a password or upgrading the account's authority. The applicant and approver of the account cannot be the same person. Additionally, Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimized permission assignment and strict behavior audit ensure that unauthorized access is not performed.	Customers should establish a management mechanism for privileged accounts to monitor the use of privileged accounts. Customers can use IAM which can implement fine-grained management of privileged accounts. Cloud Trace Service (CTS) records operations on cloud service resources so that they can be queried, audited, and traced.

5、6	changes in access rights should be processed in a timely manner. periodically user access rights and profiles should be reviewed.	Huawei Cloud has specified the maximum review period for accounts/rights at different levels. The account/right owner periodically reviews the accounts/ rights held by the account/right owner and submits a deregistration application when the user is transferred or the role changed. The management owner submits a deregistration application when the outsourced personnel leaves the site or no longer needs the account or permission. The supervisor will review whether the subordinate's account/right is proper. If the subordinate's position/ role changes, the supervisor will review whether the subordinate's account/right of the original position has been cancelled.	Customers should regularly review the account permission scope for the user accounts it is responsible for to ensure that the user permission application, change, or reclaim can be managed in a timely manner based on the identity and access control policy.
7	an audit trail of submitted, approved and processed user access requests and revocation requests should be established.	Huawei Cloud has established a periodic permission review mechanism. Operation logs are enabled for permission review to record permission addition, change, and deletion. Security personnel periodically audit permission change logs. If an uncleared resignation account is found, the security personnel will ask the system administrator to clear it.	Customers should establish an audit trail of submitted, approved and processed user access requests and revocation requests.

c	user access management should be supported by automation.	Huawei Cloud employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. All O&M accounts, device accounts, and application accounts are managed in a unified manner to ensure the end-to-end management, including user creation, authorization, authentication, and permission reclaiming.	Customers should comply with the established identity authentication and access control management policies to control user account permissions. Customers can use Identity and Access Management (IAM) of Huawei Cloud to manage user accounts that use cloud resources. Huawei Cloud IAM provides user account management services suitable for enterprise-level organizations and assigns different resources and operation rights to customers.

d	centralization of the identity and access management function.	Huawei Cloud employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. Identity and Access Management (IAM) is used to control and manage user access to cloud services. All O&M accounts, device accounts, and application accounts are managed in a unified manner to ensure the end-to-end management, including user creation, authorization, authentication, and permission reclaiming. Huawei Cloud has formulated the life cycle management of O&M accounts, It includes the administration of account registration and deletion, account owners and users, passwords, and the monitoring and auditing of account registration and deletion. Once created, new accounts are immediately scoped in for daily O&M by security administrators. All O&M, device, and application accounts are centrally managed. All accounts are centrally monitored and automatically audited through the unified audit platform. Therefore, the entire account lifecycle is well managed, from account creation, permissions granting, permissions verification and access granting, and account and permissions deletion.	Customer should use centralization of the identity and access management function. Customers can use Identity and Access Management (IAM) of Huawei Cloud to manage user accounts that use cloud resources. Huawei Cloud IAM provides user account management services suitable for enterprise-level organizations and assigns different resources and operation rights to customers.

e	multi-factor authentication for sensitive and critical systems and profiles	Huawei Cloud IAM is used to manage access and supports multi-factor authentication for login verification and operation protection. Employees need to use multi-factor authentication to determine their identity each time they log in. When employees access the Huawei Cloud office network through the Internet, they should only login through the VPN that supports the multi-factor authentication of registed and authenticated device, account and password.	Customers should have a multi-factor authentication policy for remote access. Customers can use Huawei Cloud IAM. After passing the password authentication, they will receive a one-time SMS authentication code for secondary authentication. When sensitive information such as passwords and mobile phones is modified, IAM enables multi-factor authentication by default to ensure user account security.
f	Privileges and remote access management, it should resolve:		

1	The allocation and restricted use of privileged and remote access, specifying: a. multi-factor authentication should be used for all remote access. b. multi-factor authentication should be used for privilege access on critical systems based on a risk assessment.	Huawei Cloud has defined management requirements for privileged accounts. Privileged accounts are classified and comply with management requirements during the creation, recycling, authorization, use, and deregistration of privileged accounts. Huawei employee accounts and two-factor authentication, such as USB token or smart card, are required for O&M personnel to access the Huawei Cloud management network from which systems are centrally managed. Employee accounts are used to connect securely to jump servers over remote access VPN. Both VPN gateways and bastion servers support detailed auditing of user login and access operations	Customers should establish a management mechanism for privileged accounts to monitor the use of privileged accounts. Customers can use IAM which can implement fine-grained management of privileged accounts. Cloud Trace Service (CTS) records operations on cloud service resources so that they can be queried, audited, and traced.

2、3	the periodic review of users with privileged and remote accounts. individual accountability	Huawei Cloud has defined management requirements for privileged accounts. Privileged accounts are classified and comply with management requirements during the creation, recycling, authorization, use, and deregistration of privileged accounts. Huawei Cloud emphasizes that security risks of employee cloud service accounts are controllable. Strong passwords are strictly required. Account permissions are regularly reviewed. Privileged accounts are strictly managed and reclaimed. The privileged account management system binds functional and technical accounts for daily and emergency O&M to O&M teams or individuals. Privileged or contingency accounts are granted to employees only when required by their duties. All requests for privileged or emergency accounts are reviewed and approved at multiple levels. Huawei Cloud will not access the customer's cloud environment, except in the case of maintenance failures. Huawei Cloud will use a specified tool to access the tenant's console or resource instance only after O&M personnel obtain the customer's authorization through the work order system or written authorization from the customer. Low-level logging is supported on bastion servers to ensure that all operations on the target host can be traced to any O&M personnel.	Customers should establish a management mechanism for privileged accounts to monitor the use of privileged accounts.

4	the use of non-personal privileged accounts, including: a. limitation and monitoring. b. confidentiality of passwords. c. changing passwords frequently and at the end of each session.	Once created, new accounts are immediately scoped in for daily O&M by security administrators. All O&M, device, and application accounts are centrally managed. All accounts are centrally monitored and automatically audited through the unified audit platform. Therefore, the entire account lifecycle is well managed, from account creation, permissions granting, permissions verification and access granting, and account and permissions deletion. When a user requests the use of an account, the account security administrator must start the permissions granting procedure and modify permissions after approval, providing the requestor with a new passphrase when needed. Huawei Cloud requires that account and password cannot be assigned to a specific individual. The account/right owner reviews the dedicated account he/she is responsible for, changes the password when the dedicated account is no longer needed, and notifies the new user.	Customers shall restrict and monitor the use of non-personal privileged accounts to ensure the confidentiality of passwords.

5.3.6 Application Security

To ensure that sufficient cyber security controls are formally documented and implemented for all applications, and that the compliance is monitored and its effectiveness is evaluated periodically within the financial institution.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The application cyber security standards should be defined, approved and implemented.	Huawei Cloud has formulated system development security management procedures, which define security coding specifications and application security development specifications that Huawei Cloud services must comply with during planning, design, development, deployment, O&M, and user support environments.	Customers should define and implement requirements for secure software development and implement security controls in the software development life cycle.
2	The compliance with the application security standards should be monitored.	Huawei Cloud reviews and updates the established secure system development and test procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update the requirements for secure software development periodically.
3	The effectiveness of the application cyber security controls should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established secure system development and test procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update the requirements for secure software development periodically.

4	Application development should follow the approved secure system development life cycle methodology (SDLC).	Huawei Cloud implements end-to-end management of the full lifecycle of hardware and software through a comprehensive system and process as well as automated platforms and tools. The full lifecycle includes security requirement analysis, security design, security coding and testing, security acceptance and release, vulnerability management, and etc. Huawei Cloud 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.	Customers should follow the approved secure system development life cycle methodology for application development.
5	The application security standard should include:		

a	secure coding standards.	Huawei Cloud strictly complies with the secure coding specifications released by Huawei. Before they are onboarded, 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.	Customers shall specify the software development project management methods or procedures defined in secure coding standards or specifications.

b	the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], identity and access management).	Huawei Cloud and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, Huawei Cloud runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.	Customers should ensure that the security standards for the application include cybersecurity controls

c	the segregation of duties within the application (supported with a documented authorization matrix).	Huawei Cloud complies with the separation of duties (SOD) and rights checks and balances principles to separate incompatible responsibilities to achieve proper rights division. In addition, the SOD management matrix is developed to help implement the SOD management principles. Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, data transmission channel approval, and auditing. Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimized permission assignment and strict behavior audit ensure that unauthorized access is not performed.	Customers should ensure that the security standards for the application include the segregation of duties within the application.
d	the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage).	Huawei Cloud uses multi-layered protection mechanisms and measures to safeguard application services provided on the public network, including the user identity authenticated and authorized through the IAM service, API calls must use TLS-based encryption to ensure the confidentiality of data during transit. Secure encryption channels (e.g. HTTPS) are used during information transmission, and stored static data is encrypted and protected by secure encryption algorithms to ensure the confidentiality of data in different states. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.	Customers should ensure that the data in the application is protected.

e	vulnerability and patch management.	Huawei Cloud has established a security vulnerability management process, which standardizes the closed-loop process of warning, assessment, and fixing of security vulnerabilities in Huawei Cloud systems. It also requires regular critical security patches to reduce vulnerability risks and specifies the requirements of vulnerabilities classification, responsibilities allocation, and vulnerability handling. Additionally, Huawei Cloud has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures. For vulnerabilities that may affect customer service, Huawei Cloud will disclose the vulnerabilities to customers by the Saudi Arabia business service support team, including vulnerability details, vulnerability principle analysis, vulnerability impact scope, vulnerability prevention measures, and vulnerability resolution methods.	Customers should establish effective vulnerability management mechanisms and conduct vulnerability identification and risk assessment for all technology assets.

f	back-up and recovery procedures.	Huawei Cloud has formulated and implemented backup and redundancy policies, including development and test environment, code document version management, backup and redundancy of the production system, tool software and security equipment. Huawei Cloud has formulated data backup specifications to standardize the data backup format, backup time, backup content, and policy. In addition, Huawei Cloud standardizes the formulation of service recovery policies to ensure that services can be recovered to an acceptable level within the recovery time objective.	Customers should establish a security management procedure for backup and recovery that defines the backup requirements for information, software and system.
g	periodic cyber security compliance review.	Huawei Cloud has established a formal and regular audit plan, including continuous and independent internal and external assessments. The internal assessment continuously tracks the effectiveness of security control measures, and the external assessment audits as independent auditors to assess the running status of the company's cyber security control system, and evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators.	Customers should conduct periodic cybersecurity compliance reviews to determine the compliance and effectiveness of cybersecurity controls.

5.3.7 Change Management

To ensure that all change in the information assets within the financial institution follow a strict change control process.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The change management process should be defined, approved and implemented.	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.	Customers should establish a change management procedure to identify, classify, and prioritize changes based on the importance of information assets.
2	The compliance with the change management process should be monitored.	Huawei Cloud reviews and updates the regulations and procedures related to change management annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should continuously review and optimize the change management procedures as well as the controls used periodically.
3	The effectiveness of the cyber security controls within the change management process should be measured and periodically evaluated.	Huawei Cloud reviews and updates the regulations and procedures related to change management annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should continuously review and optimize the change management procedures as well as the controls used periodically.
4	The change management process should include:		

a	cyber security requirements for controlling changes to information assets, such as assessing the impact of requested changes, classification of changes and the review of changes.	Huawei Cloud has developed the change management regulations and procedures, which define different change management processes for different change types, including change application, review, and implementation. Each change must be reviewed in multiple phases, and changes are classified based on factors such as change urgency.	Customers shall establish a change management procedure to identify, classify, and prioritize changes based on the importance of information assets.
b	security testing, which should (if applicable) include:		
1	penetration testing.	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.	Customers should conduct penetration testing on a regular basis.
2	code review if applications are developed internally	Huawei Cloud introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/ Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code related issues that can extend rollout time coding.	Customers should conduct code reviews for internally developed applications.

3、4	code review of externally developed applications and if the source code is available. a code review report (or equivalent, such as an independent assurance statement) in case the source code cannot be provided.	Huawei Cloud ensures the secure introduction and use of open source and third party software based on the principle of strict entry and wide use. Huawei Cloud has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. For example, cybersecurity assessment requirements are added to open source software selection in the selection analysis phase to strictly control the selection. During the use of third-party software, carry out related activities by taking the third-party software as part of services or solutions, and focus on the assessment of the integration of open source, third-party, and Huawei-developed software, or whether new security issues are introduced when independent third-party software is used in solutions.	Customers should ensure code security for externally developed applications.

c、d、e	approval of changes by the business owner. approval from the cyber security function before submitting to Change Advisory Board (CAB). approval by CAB.	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.	Customers should establish a formal change approval mechanism. The change can be made only after the business owner, cyber security functional department, and the change committee authorizes and approves the change.
f	post-implementation review of the related cyber security controls.	Huawei Cloud has established formal internal testing and acceptance measures to ensure that only appropriate and authorized changes are released to the production environment. Before the change into the production environment, submit an internal acceptance test report and describe the test acceptance method in the change management system to ensure that all types of change requirements are tested before the change into the production environment to check whether the cyber security control is effective. After the change is implemented, special personnel are assigned to verify the change to ensure that the change achieves the expected purpose.	Customers reviews the cybersecurity controls for the implementation of the change.

g	development, testing and implementation are segregated for both the (technical) environment and involved individuals.	Huawei Cloud has established a formal environment isolation mechanism to logically isolate the development, test, and production environments, improving self-protection and fault tolerance capabilities against external intrusions and internal violations, and reducing risks of unauthorized access or change to the operating environment. Do not connect the network between the test environment and the production environment without authorization to avoid security risks in the production environment due to intrusion of the test environment.	The customer should ensure that their development, test, and production environments are isolated from each other and that the use of the different environments is strictly controlled.
h	the procedure for emergency changes and fixes.	Huawei Cloud has developed a standard emergency change management process. If an emergency change affects users, they will communicate with users in advance by means of announcements, emails, telephone calls, and meetings within the specified time limit. If an emergency change does not meet the specified notification time limit, the change will be escalated to Huawei Cloud senior management and will be notified to users in a timely manner after the change is implemented. In addition, if the impact in production environment caused by changes meets the event standard, Huawei Cloud requires immediate report to the emergency team for quick fault rectification. Records are kept for emergency changes. The old program version and data are retained before the change is implemented. During the change, two-person operations are used to ensure the smooth progress of the change and minimize the impact on the production environment.	Customer should develop and implement a process for emergency changes and fixes.

i	fall-back and roll-back procedures.	The change application must submit a change plan, which must provide a rollback plan and a rollback method. If the impact on the production environment is affected, the rollback will be initiated according to the change plan as soon as possible.	Customers should develop and implement change fallback and rollback procedures.

5.3.8 Infrastructure Security

To support that all cyber security controls within the infrastructure are formally documented and the compliance is monitored and its effectiveness is evaluated periodically within the financial institution.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The infrastructure security standards should be defined, approved and implemented.	Huawei Cloud complies with IT security standards established by Huawei, which specify security control requirements for preventing unauthorized changes or malicious intrusions to infrastructure, including harmful code protection, malware protection, virus protection, media management, and patch management. Huawei Cloud deploy a series of cybersecurity protection equipment such as NDR and firework and implement effective security measures to ensure the security of information processing facilities. Huawei Cloud considers infrastructure security to be a core component of its multi-dimensional full-stack cloud security framework. On the secure infrastructure base built through Huawei Cloud, tenants can be more confident in moving their business to Huawei Cloud and leveraging our cloud services to grow their business.	Customers should define and implement infrastructure security standards.

2	The compliance with the infrastructure security standards should be monitored.	Huawei Cloud regularly reviews and updates infrastructure protection policies and processes. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should periodically review and update infrastructure security standards as scheduled.
3	The effectiveness of the infrastructure cyber security controls should be measured and periodically evaluated.	Huawei Cloud regularly reviews and updates infrastructure protection policies and processes. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should periodically review and update infrastructure security standards as scheduled.

4	The infrastructure security standards should cover all instances of infrastructure available in the main datacenter(s), the disaster recovery data site(s) and office spaces.	Huawei Cloud has developed comprehensive infrastructure security standards, covering security design and practices in physical environment, network, cloud platform, application, and data. In addition, Huawei Cloud complies with IT security standards established by Huawei, which specify security control requirements for preventing unauthorized changes or malicious intrusions to infrastructure, including harmful code protection, malware protection, virus protection, media management, and patch management. Security standards for office terminals, office devices, emails, and files are followed with the Huawei's security standards. In addition, Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the multiple region and multiple-AZ data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. The two sites serve as each other's DR site and keeps each other backed up. Their security measures remain the same.	Customers should ensure that security standards for the infrastructure cover all available infrastructure instances in the primary data center, disaster recovery data site, and office space.

5	The infrastructure security standards should cover all instances of infrastructure (e.g., operating systems, servers, virtual machines, firewalls, network devices, IDS, IPS, wireless network, gateway servers, proxy servers, email gateways, external connections, databases, file-shares, workstations, laptops, tablets, mobile devices, PBX).	Huawei Cloud has developed comprehensive infrastructure security standards, covering security design and practices in physical environment, network, cloud platform, application, and data. In addition, Huawei Cloud complies with IT security standards established by Huawei, which specify security control requirements for preventing unauthorized changes or malicious intrusions to infrastructure, including harmful code protection, malware protection, virus protection, media management, and patch management. Security standards for office terminals, office devices, emails, and files are followed with the Huawei's security standards.	Customers should ensure that infrastructure security standards cover all instances of infrastructure.
6	The infrastructure security standard should include:		
a	the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance).	Huawei Cloud implements a series of network security controls on the physical environment, network, cloud platform, application, and data in its security protection system to ensure infrastructure security design and practice. In addition, Huawei Cloud establishes unified baseline configuration standards for server operating systems, database management systems, and network devices that support service operation to implement unified management of service baseline configurations, specify security configuration requirements for systems/ components in the production environment, and ensure effective execution and continuous improvement of security configurations.	Customers should comply with the network security requirements of infrastructure security standards and implement effective network security control.

b	the segregation of duties within the infrastructure component (supported with a documented authorization matrix)	Huawei Cloud complies with the separation of duties (SOD) and rights checks and balances principles to separate incompatible responsibilities to achieve proper rights division. In addition, the SOD management matrix is developed to help implement the SOD management principles. Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, data transmission channel approval, and auditing. Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and responsibilities can only perform specific operations on authorized targets. Minimize permission assignment and strict behavior audits to ensure that people do not access without authorization.	Customers should ensure that the security standards for the infrastructure include segregation of duties for infrastructure components.

c	the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage).	Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks. In addition, Huawei Cloud provides multi-layer protection measures. For example, access control and border protection technologies are used to implement coordinated protection against external attacks and strictly implement corresponding management and control measures to ensure Huawei Cloud security. Based on business functions and network security risks, the Huawei Cloud data center network is mapped into different security zones to achieve network isolation using both physical and logical controls to Improves the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. Huawei Cloud data center network is mapped into different security zones, including: DMZ zone, Public services zone, Point of Delivery (POD), Object - Based Storage (OBS), and Operations Management (OM). In addition to the abovementioned security zoning for every Huawei Cloud data center's network, distinct security levels within different security zones are also defined for Huawei Cloud. Attack surfaces and security risks are determined based on different business	Customers should implement protection of data that complies with the classification plan to prevent unauthorized access and data leakage.

		functions. For example, security zones that are directly exposed to the Internet have the highest security risks, whereas the O&M zone that exposes no interface to the Internet therefore has a much smaller attack surface, lower security risks, and less challenging to manage. The internal network is isolated from the external network and abnormal traffic cleaning is implemented. Huawei Cloud will not access the customer's cloud environment except during fault maintenance. O&M personnel can access tenant consoles or resource instances only after obtaining the customer's authorization through the work order system or in written form. Operations beyond the customer's authorization or prohibited high-risk operations are prohibited, or deploy and run software that is not authorized by the customer on the customer's network. In addition, the O&M platform supports strong log audit to ensure that O&M personnel's operations on the target host can be located to individuals, preventing unauthorized access and data leakage.	

d	the use of approved software and secure protocols.	Huawei Cloud formulates and implements desktop terminal service software standards and open-source software lists, and only standard operating systems and software applications defined in the list can be used. In addition, Huawei Cloud restricts the use of high-risk ports and high-risk protocols by configuring firewall policies. Moreover, Huawei Cloud has developed a product communication matrix, which maintains available communication ports. Ports must be within a reasonable range. Ports not listed in the matrix must be disabled and verified by the port scanning tool.	Customers should ensure that approved software and security protocols are used.
e	segmentation of networks.	Huawei Cloud data center network is mapped into different security zones, including: DMZ zone, Public services zone, Point of Delivery (POD), Object - Based Storage (OBS), and Operations Management (OM). In addition to the abovementioned security zoning for every Huawei Cloud data center's network, distinct security levels within different security zones are also defined for Huawei Cloud. Attack surfaces and security risks are determined based on different business functions. For example, security zones that are directly exposed to the Internet have the highest security risks, whereas the O&M zone that exposes no interface to the Internet therefore has a much smaller attack surface, lower security risks, and less challenging to manage.	Customers need to divide and isolate their networks into security zones and strictly control access between different security zones.

f	malicious code/ software and virus protection (and applying application whitelisting and APT protection).	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 (WAF), anti-virus software, and HIDS host-based intrusion detection system for vulnerability management of system components and networks. The IPS intrusion prevention system can detect and prevent potential network intrusion activities; Web application firewalls are deployed at the network boundary to protect the security of application software and protect it from external SQL injection, CSS, CSRF and other application oriented attacks; Anti-virus software provides virus protection and firewall in Windows system; HIDS host-based intrusion detection system protects the security of cloud servers, reduces the risk of account theft, provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web tamper protection.	Customers should implement security management measures to detect and prevent malware and malicious viruses on information systems and information processing facilities. 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.

g	vulnerability and patch management.	Huawei Cloud has established a security vulnerability management process, which standardizes the closed-loop process of warning, assessment, and fixing of security vulnerabilities in Huawei Cloud systems. It also requires regular critical security patches to reduce vulnerability risks and specifies the requirements of vulnerabilities classification, responsibilities allocation, and vulnerability handling. Additionally, Huawei Cloud has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures.	Customers should establish effective vulnerability management mechanisms and conduct vulnerability identification and risk assessment for all technology assets.

h	DDOS protection (where applicable). this should include: 1. the use of scrubbing services. 2. specification of the bandwidth agreed. 3. 24x7 monitoring by Security Operating Center (SOC), Service Provider (SP) and scrubbing provider. 4. testing of DDOS scrubbing (minimum twice a year). 5. DDOS services should be implemented for the main datacenter(s) as well as the disaster recovery site(s).	1. Huawei Cloud deploys DoS/ DDoS prevention and cleaning layer, next-generation firewall, intrusion prevention system layer, and web application firewall layer at the network border. Huawei Cloud defends against heavy traffic attacks from outside the cloud platform or from other virtual machines inside the platform by limiting the number of connection traces on virtual ports. Such attacks generate a large number of connection tracking entries, which, if not limited, will exhaust the connection tracking table resources, resulting in the inability to receive new connection requests and eventually causing business and management traffic interruption. 2. Huawei in-house-developed enterprise-grade anti-DDoS appliances, which are deployed at the perimeter of each cloud data center network, detect and scrub abnormal traffic and mega load attacks. Anti-DDoS can defend against DDoS attacks at a rate of 2 Gbit/s, up to 5 Gbit/s. The traffic peak rate is 2 Gbit/s, that is, the maximum anti-DDoS traffic. 3. In addition, given the professionalism and urgency to handle security incidents, Huawei Cloud has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. Huawei Cloud annually tests information security incident management procedures. 4. Huawei Cloud has established a periodic vulnerability scanning mechanism, and	Customers should implement DDoS protection measures, which should explicitly use traffic cleaning services, standardize protected traffic, and monitor it 24/7, perform testing of DDoS services, and implement DDoS services at the primary data center and disaster recovery site. Huawei Cloud provides anti-DDoS traffic cleaning services for customers. Customers can deploy anti-DDoS traffic cleaning devices in their data center network egress areas. Anti-DDoS devices monitor service traffic from the Internet to ECSs, Elastic Load Balance, and bare metal server in real time to detect abnormal DDoS attack traffic in a timely manner. Cleans attack traffic based on the configured protection policy without affecting services.

		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. In addition, Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the multiple region and multiple-AZ data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. The two sites serve as each other's DR site and keeps each other backed up. Their security measures remain the same. Therefore, HUAWEI CLOUD deploys the DDoS service in both the primary data center and DR site.	

i	back-up and recovery procedures.	Huawei Cloud has formulated and implemented backup and redundancy policies, including development and test environment, code document version management, backup and redundancy of the production system, tool software and security equipment. Huawei Cloud has formulated data backup specifications to standardize the data backup format, backup time, backup content, and policy. In addition, Huawei Cloud standardizes the formulation of service recovery policies to ensure that services can be recovered to an acceptable level within the recovery time objective.	Customers should establish a security management procedure for backup and recovery that defines the backup requirements for information, software and system.
j	periodic cyber security compliance review.	Huawei Cloud has established a formal and regular audit plan, including continuous and independent internal and external assessments. The internal assessment continuously tracks the effectiveness of security control measures, and the external assessment audits as independent auditors to assess the running status of the company's cyber security control system, and evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators.	Customers should conduct periodic cybersecurity compliance reviews to determine the compliance and effectiveness of cybersecurity controls.

5.3.9 Cryptography

To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	A cryptographic security standard should be defined, approved and implemented.	Huawei Cloud formulates and implements cryptographic algorithm application specifications. This document describes how to select secure encryption algorithms and the rules for using secure encryption algorithms. It also provides guidance on the correct use of cryptographic algorithms with application examples. Huawei Cloud uses the AES encryption method widely used in the industry to encrypt data on the platform, and uses the high-version TLS encryption protocol to secure data during the transmission processes, ensuring data confidentiality in different states. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.	Customers should establish cryptography management procedures and ensure the proper and effective use of cryptographic technology to protect the confidentiality, authenticity and integrity of information.
2	The compliance with the cryptographic security standard should be monitored.	Huawei Cloud reviews and updates the established cryptographic algorithm application standards and key management security procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update the cybersecurity requirements for encryption security standards as well as the effectiveness of the implemented cryptographic solutions periodically.
3	The effectiveness of the cryptographic security controls should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established cryptographic algorithm application standards and key management security procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update the cybersecurity requirements for encryption security standards as well as the effectiveness of the implemented cryptographic solutions periodically.

4	The cryptographic security standard should include:		
a	an overview of the approved cryptographic solutions and relevant restrictions (e.g., technically, legally).	Huawei Cloud implements the cryptographic algorithm application specification maintained by Huawei Cyber Security Competence Center, which contains the standardized information list of common cryptographic algorithms and solutions. This list has been referenced to widely used standards and best practices in the industry to guide products to correctly select and use cryptographic algorithms.	Customers should consider using industry-accepted encryption algorithms and key management mechanisms when using encryption to protect data.

b	the circumstances when the approved cryptographic solutions should be applied.	Huawei Cloud has established encryption policies and key management procedures to protect data on technical devices, and specifies the encryption levels and encryption methods. Huawei Cloud uses the industry's widely used AES strong encryption method to encrypt data on the platform. In the scenario where data is transmitted between customers and servers and between servers of the Huawei Cloud via common information channels, data in transit is protected as follows: 1. Virtual private network (VPN): VPN is used to establish a secure encrypted communication channel that complies with industry standards between a remote network and a tenant VPC. Currently, Huawei Cloud uses IPsec VPN together with Internet Key Exchange (IKE) to encrypt the data transport channel and ensure transport security. 2. Application layer TLS and certificate management: Huawei Cloud supports data transmission in REST and Highway modes. Both REST and Highway modes support TLS 1.2 for data in transit encryption and X. 509 certificate-based identity authentication of destination websites. In addition, the infrastructure storage and database provided by Huawei Cloud have data backup strategies. The backup data copies and data use the same data security measures. For example, EVS provides secure encryption algorithms (AES-256) and functions, OBS provides server-side encryption and anti-leeching functions, and RDS provides storage encryption mechanisms. By integrating with the data encryption service,	Customers should define a policy for the use of cryptographic, considering the type, strength and quality of encryption algorithms for in-transit and static data, based on the level of classification of data and information. Customers can encrypt data through Huawei Cloud's data storage and encryption service. Huawei Cloud encapsulates complex data encryption and decryption, and key management logic, which makes the operation of customer's data encryption easy. Currently, services including Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or serverside encryption functions and encrypt data using high-

		backup data can be encrypted and stored conveniently and quickly, ensuring security of the backup data.	strength algorithms. For data in transmission, when customers provide Web site services through the Internet, they can use certificate management services provided by the Huawei Cloud United Global Well-known Certificate Service Provider. By applying for and configuring certificates for Web sites, the trusted identity authentication of Web sites and secure transmission based on encryption protocols are realized. Customers can also purchase certificates on third-party platforms.

c	the management of encryption keys, including lifecycle management, archiving and recovery.	Huawei Cloud has formulated and implemented key management security specifications to manage security in each phase of the key lifecycle, and specifies security management requirements for key generation, transmission, use, storage, update, backup and recovery, and destruction.	Customers should establish a key management mechanism to process the generation, protection, archiving, restoration, and destruction of encryption keys so that data confidentiality and integrity are not compromised. Huawei Cloud provides the Data Encryption Service (DEW) for customers. The DEW key management function enables you to centrally manage keys throughout the lifecycle. Without authorization, no one except the customer cannot obtain a key to decrypt data, ensuring data security on the cloud. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. Huawei Cloud uses the hardware security module (HSM) to create and manage keys for customers. HSM has FIPS140-2 (level

			2 and level 3) mainstream international security certification, helping users meet data compliance requirements and prevent intrusion and tampering. Even Huawei O&M personnel cannot steal customer root keys. DEW allows customers to import their own keys as CMKs for unified management, facilitating seamless integration and interconnection with customers' existing services. In addition, Huawei Cloud uses customer master key online redundancy storage, multiple physical offline backups of root keys, and periodic backups to ensure key persistence.

5.3.10 Bring Your Own Device (BYOD)

To ensure that business and sensitive information of the financial institution is securely handled by staff and protected during transmission and storage, when using personal devices.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The BYOD cyber security standard should be defined, approved and implemented.	Huawei Cloud has formulated regulations on mobile device management to implement unified management of mobile computing devices. This document specifies the principles, responsibilities, rights requirements, and security requirements for device management, network access requirements, and penalties for violations of mobile devices.	Customers should develop mobile device security and BYOD management policies.
2	The compliance with the BYOD cyber security standard should be monitored.	Huawei Cloud reviews and updates the regulations and policy processes related to removable office terminal annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should regularly review and optimize removable terminal and BYOD requirements and the effectiveness of processes.
3	The effectiveness of the BYOD cyber security controls should be measured and periodically evaluated.	\Huawei Cloud reviews and updates the regulations and policy processes related to removable office terminal annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should regularly review and optimize removable terminal and BYOD requirements and the effectiveness of processes.
4	The BYOD standard should include:		

a	responsibilities of the user (including awareness training).	To develop employees' security awareness, Huawei Cloud provides continuous training for on-the-job employees and special information security training plans. Awareness education includes but is not limited to on-site speeches and online video courses.	The customer should securely erase organizational data and information stored on mobile devices and BYOD after the device is lost, stolen, or terminated/ separated from the organization.
b	information regarding the restrictions and consequences for staff when the financial institution implements cyber security controls on their personal devices. for example when using modified devices (jailbreaking), terminating the employment or in case of loss or theft of the personal device.	When employees resign or transfer to another position, the hard disk of the office computer must be formatted. If confidential and top secret information is involved, they should ensure that the deleted data cannot be recovered. In addition, employees should take the initiative to uninstall the company application on BYOD and clear the company data in a timely manner. If the device is lost or stolen, the employee must report to the business supervisor and the information security department, remotely erase the company data and cancel the device binding.	Customers should securely erase organizational data and information stored on mobile devices and BYOD after the device is lost, stolen, or terminated/ separated from the organization.

c	the isolation of business information from personal information (e.g., containerization).	Huawei Cloud has established encryption policies and key management mechanism to protect data on technical devices, and has specified the authority and duty assignment of personnel, encryption levels, and encryption methods. In addition, for different levels of data, electronic streams or emails containing confidential data are restricted from being released to applications on the mobile BYOD side, and organizational data and information on BYOD do not involve Huawei's core information assets.	The customer should ensure that data and information assets stored in the device are encrypted.
d	the regulation of corporate mobile applications or approved “public” mobile applications.	Huawei Cloud has formulated security management regulations for office applications, which specify that enterprise office application systems are used only for purposes authorized by Huawei business or related management, and have the right to monitor the use of office application systems to ensure the security of office application systems.	Customers should regulate mobile applications within their organization.

e	the use of mobile device management (MDM). applying access controls to the device and business container and encryption mechanisms on the personal device (to ensure secure transmission and storage).	Huawei Cloud uses the mobile device management (MDM) system to implement unified management of mobile devices, record and maintain an inventory of all end users and mobile devices, and classify, monitor, and manage mobile devices. Huawei Cloud has established encryption policies and key management mechanism to protect data on technical devices, and has specified the authority and duty assignment of personnel, encryption levels, and encryption methods. In addition, for different levels of data, electronic streams or emails containing confidential data are restricted from being released to applications on the mobile BYOD side, and organizational data and information on BYOD do not involve Huawei's core information assets.	Customers should use mobile device management tools, and apply encryption mechanisms on the personal device.

5.3.11 Secure Disposal of Information Assets

To ensure that the financial institution’s business, customer and other sensitive information are protected from leakage or unauthorized disclosure when disposed.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The secure disposal standard and procedure should be defined, approved and implemented.	Huawei Cloud has formulated asset management procedures, which specify the classification and grading methods of information assets and the authorization rules that should be followed for various types of assets. In addition, Huawei Cloud has established information asset confidentiality management requirements, which specify the confidentiality measures that Huawei Cloud should take for information assets at different levels, and standardize the use of assets to ensure that the company's assets are properly protected and shared and ensure assets are protected at the appropriate level according to their importance to the organization. Huawei Cloud uses the Cloud Asset Management (CAM) system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and form an asset list.	Customers should define and develop cybersecurity requirements for information and technology asset management based on different levels of asset classification to ensure the appropriate level of asset protection
2	The compliance with the secure disposal standard and procedure should be monitored.	Huawei Cloud reviews and updates asset disposal processes annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should regularly review and optimize asset disposal requirements and the effectiveness of processes.

3	The effectiveness of the secure disposal cyber security controls should be measured and periodically evaluated.	Huawei Cloud reviews and updates asset disposal processes annually. In addition, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure the implementation of security governance policies, standards, regulations, and specific measures in the processes of each business domain.	Customers should regularly review and optimize asset disposal requirements and the effectiveness of processes.
4	Information assets should be disposed in accordance with legal and regulatory requirements, when no longer required (i.e. meeting data privacy regulations to avoid unauthorized access and avoid (un)intended data leakage).	For storage media assets that store Huawei information, Huawei Cloud has formulated and implemented relevant media management regulations, in which the media are cleared and scrapped according to the classification. Huawei Cloud achieves data cleaning, disk demagnetization through a variety of ways, and records the destruction operation. Dedicated personnel manage devices that contain storage media on Huawei Cloud. After the devices are used, dedicated personnel format the devices. When a storage media that stores HUAWEI's confidential information is scrapped, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting.	Customers should define and implement asset disposal processes to handle the disposition of information assets to prevent unauthorized disclosure or modification.

5	Sensitive information should be destroyed using techniques to make the information non-retrievable (e.g., secure erase, secure wiping, incineration, double crosscut, shredding).	Huawei cloud storage media standards specify that media containing Huawei confidential information or personal data must be used before being processed or used for purposes irrelevant to Huawei's services, dedicated personnel must ensure that the information stored on the media is erased and cannot be recovered. The disposal methods include degaussing, physical destruction, or low-level formatting. If a physical storage medium is to be disposed, the destruction of physical storage media must be carried out under the full supervision of Huawei employees. Huawei Cloud clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.	Customer should ensure that the sensitive information should be destroyed using techniques to make the information non-retrievable.

6	The financial institution should ensure that third party service providers used for secure disposal, transport and storage comply with the secure disposal standard and procedure and the effectiveness is periodically measured and evaluated.	As a cloud service provider of financial institutions, Huawei Cloud has formulated and implemented media management regulations, which specify: • Huawei Cloud requires that storage media containing Huawei confidential information must be marked. Confidential data shall be marked or labeled according to the data security level, and the security level shall be stated. Labels must be attached to the exterior of media in transit or facilities authorized to store the media, and to the exterior of locked containers used for transporter media. • Huawei Cloud requires storage media to be stored in a controlled access area or in a locked cabinet. When a storage media enters or exits a controlled area, the detailed information from outbound to inbound must be reconciled and tracked in a closed-loop manner. • Huawei Cloud ensures that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Customers should periodically review and evaluate third-party service providers for compliance with secure disposal standards.

5.3.12 Cyber Security Event Management

To ensure timely identification and response to anomalies or suspicious events within regard to information assets.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The security event management process should be defined, approved and implemented.	Huawei Cloud has established an incident handling process and complies with the incident response process when a security incident occurs. (Identification, assessment, decision making, and execution of emergency response processing). At the same time, Huawei Cloud standardizes security incident escalation principles. If a new risk is identified during incident source tracing, the severity of a new security incident needs to be determined based on the accumulated result of the incident and re-rated. The roles and responsibilities are clearly defined for each activity during the incident response process.	Customers should develop a cybersecurity incidents management strategy, establish a security incidents escalation and decision process, and implement appropriate response plans and communication strategies.
2	The effectiveness of the cyber security controls within the security event management process should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established security incidents management standards and procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should periodically review and update security requirements for cybersecurity incidents and threats.

3	To support this process a security event monitoring standard should be defined, approved and implemented. a. the standard should address for all information assets the mandatory events which should be monitored, based on the classification or risk profile of the information asset.	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 incidents analysis and processing platform in real-time. Huawei Cloud security incident response team is responsible for incident monitor and record, and assess whether a security incident is, also they track and manage the collected security incident by unified management to ensure security incident can be fixed in time. 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.	Customers should measure and monitor cybersecurity incidents.
4	The security event management process should include requirements for:		
a	the establishment of a designated team responsible for security monitoring (i.e., Security Operations Center (SOC)).	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.	Customers should establish a designated team for security monitoring.

b	skilled and (continuously) trained staff.	Huawei's technical security personnel consists of some of the world's leading experts and specialists in information security, product security, application security, system security, network security, cloud service security, O&M security, and privacy protection. In addition, Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. The training frequency for general employees is at least once a year, and the training frequency for core employees is higher.	Customers should hire skilled and trained staff.
c	a restricted area to facilitate SOC activities and workspaces.	Huawei Cloud O&M center ensures O&M security through physical measures such as access control management system, video surveillance system, independent area, fire prevention and power failure prevention. The O&M center is isolated from the open office area, and the office area is divided into multiple security zones of different levels for management, and grant access based on job needs.	Customers should set up a restricted area to facilitate SOC activities and workspaces.
d	resources required continuous security event monitoring activities (24x7).	To ensure the professionalism and urgency security event handling, Huawei Cloud has a 24/7 professional security event response team, and a corresponding security expert resource pool.	Customers should monitor security event for resources continuously.

e	detection and handling of malicious code and software.	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 (WAF), anti-virus software, and HIDS host-based intrusion detection system for vulnerability management of system components and networks. The IPS intrusion prevention system can detect and prevent potential network intrusion activities; Web application firewalls are deployed at the network boundary to protect the security of application software and protect it from external SQL injection, CSS, CSRF and other application oriented attacks; Anti-virus software provides virus protection and firewall in Windows system; HIDS host-based intrusion detection system protects the security of cloud servers, reduces the risk of account theft, provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web tamper protection.	Customers should implement security management measures to detect and prevent malware and malicious viruses. 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.

f	detection and handling of security or suspicious events and anomalies.	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 incidents analysis and processing platform in real-time. Huawei Cloud security incident response team is responsible for incident monitor and record, and assess whether a security incident is, also they track and manage the collected security incident by unified management to ensure security incident can be fixed in time.	Customers should follow the established cybersecurity incidents management procedure, continuously monitor and analyze the security logs of each system, and detect and respond to security events and incidents in a timely manner. Log Tank Service (LTS) on Huawei Cloud collects, queries, and stores logs in real time. It records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. 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.

g	deployment of security network packet analysis solution.	Huawei Cloud has implemented comprehensive malware and virus protection mechanisms for the cloud platforms. Huawei Cloud uses IPS intrusion prevention system, Web Application Firewall (WAF), anti-virus software, and HIDS host-based intrusion detection system for vulnerability management of system components and networks. The IPS intrusion prevention system can detect and prevent potential network intrusion activities; Web application firewalls are deployed at the network boundary to protect the security of application software and protect it from external SQL injection, CSS, CSRF and other application oriented attacks; Anti-virus software provides virus protection and firewall in Windows system; HIDS host-based intrusion detection system protects the security of cloud servers, reduces the risk of account theft, provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web tamper protection.	Customers should deploy security network packet analysis solution.

h	adequately protected logs.	Security measures are taken to prevent log tampering to enable compliance and backtracking of network security events. To ensure log data security, security logs are backed up or archived in a unified manner, and in accordance with data security management requirements, applications and permissions for security log use are restricted, and only authorized personnel are allowed to query security logs for necessary reasons to ensure controlled use of. Huawei Cloud complies with legal requirements and has a centralized and complete log audit system with powerful data retention and query capabilities to ensure that all log content is kept for more than 6 months.	Customer should protect log information and logging facilities from unauthorized access and tampering.
i	periodic compliance monitoring of applications and infrastructure cyber security standards.	Huawei Cloud has established a formal and regular audit plan, including continuous and independent internal and external assessments. The internal assessment continuously tracks the effectiveness of security control measures, and the external assessment audits as independent auditors to assess the running status of the company's cyber security control system, and evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators.	Customers should conduct periodic cybersecurity compliance reviews to determine the compliance and effectiveness of cybersecurity controls.

j	automated and centralized analysis of security loggings and correlation of event or patterns (i.e., Security Information and Event Management (SIEM)).	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 to ensure backtracking of cyber security events. Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system administrator periodically checks the collection status and storage status of the security logs to ensure the availability of security logs. 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 incidents analysis and processing platform in real-time.	Customers should automatically and centrally analyze security logs and correlation of event or patterns, and report cyber security events in a timely manner. Log Tank Service (LTS) on Huawei Cloud collects, queries, and stores logs in real time. It records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. 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.

k	reporting of cyber security incidents.	Huawei Cloud reviews and summarizes the impact and handling processes of security incidents, and informs and reports to the corresponding affected users and regulatory departments as required. Huawei Cloud has developed a complete process for incident management and notification. If an incident occurs on the Huawei Cloud Base Platform, relevant personnel will analyze the impact of the incident according to the process. If the incident has or will have an impact on the cloud service customers, Huawei Cloud will start to notify customers of the incident. The contents of the notice include but are not limited to description of the incident, the cause, impact, measures taken by Huawei Cloud, and measures recommended for customers.	Customers should specify the process for reporting cyber security incidents.
l	independent periodic testing of the effectiveness of the security operations center (e.g., redteaming).	To meet customers' compliance requirements, Huawei Cloud regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services, 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. In addition, Through the adoption of industry best practices, a platform for practicing cybersecurity field exercises has been developed with a scenario-based real world environment for employees to conduct red team and blue team exercises, and to facilitate participation in such exercises and exchanges among employees. This platform helps improve employees' overall skill level when it comes to hands-on security techniques.	Customers should conduct the independent periodic testing of the effectiveness of the security operations center.

5.3.13 Cyber Security Incident Management

To ensure timely identification and handling of cyber security incidents in order to reduce the (potential) business impact for the financial institution

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security incident management process should be defined, approved, implemented and aligned with the enterprise incident management process.	Huawei Cloud has developed a mechanism for internal security incident management, standardized security incidents response operations, and clarified classification and escalation principle of security incidents mechanisms. The roles and responsibilities are clearly defined for each activity during the incident response process.	Customers should develop a cybersecurity incidents management strategy, establish a security incidents escalation and decision process, and implement appropriate response plans and communication strategies.
2	The effectiveness of the cyber security controls within the cyber security incident management process should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established security incidents management standards and procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should periodically review and update security requirements for cybersecurity incidents and threats.

3	The standard should address the mandatory and suspicious security events which should be responded to.	Huawei Cloud has established an incident handling process and complies with the incident response process when a security incident occurs. (Identification, assessment, decision making, and execution of emergency response processing). At the same time, Huawei Cloud standardizes security incident escalation principles. If a new risk is identified during incident source tracing, the severity of a new security incident needs to be determined based on the accumulated result of the incident and re-rated. In addition, Huawei Cloud has developed a complete incident management process. Incidents are prioritized and different processing time limits are defined according to the impact and scope of each incident. Huawei Cloud will respond to and resolve the incident within a specified time limit according to the priority of the incident, to minimize the impact of the incident on cloud service customers.	Customers should ensure that the cybersecurity incident standard can address the mandatory and suspicious security events which should be responded to.
4	The security incident management process should include requirements for:		
a	the establishment of a designated team responsible for security incident management.	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.	Customers should establish a designated team responsible for security incident management.

b	skilled and (continuously) trained staff.	Huawei's technical security personnel consists of some of the world's leading experts and specialists in information security, product security, application security, system security, network security, cloud service security, O&M security, and privacy protection. Huawei Cloud annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate.	Customers should hire skilled and trained staff.
c	sufficient capacity available of certified forensic staff for handling major incidents (e.g., internal staff or contracting an external forensic team).	Huawei Cloud annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate, to ensure timely handling of major incidents. In addition, Huawei Cloud has developed security incident emergency handling process and response process. When a server or application is suspected to be intruded, security responders collect evidence for analysis. 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.	Customers should ensure their certified forensic staff have sufficient capacity to handling major incidents

d	a restricted area to facilitate the computer emergency response team (CERT) workspaces.	Huawei Cloud has formulated the operation regulations for war rooms, which specify that each business team must maintain an office space isolated from the office area for emergency response and handling of security incidents. In addition, the Huawei Cloud war room operation specifications specify the key activity processes of the war room, such as initiation, commanding, reporting, and closure, to provide guidance for critical incident response and recovery on the production environment.	Customers should set up a restricted area to facilitate the computer emergency response team (CERT) workspaces.
e	the classification of cyber security incidents.	Huawei Cloud has developed a complete incident management process. Incidents are prioritized and different processing time limits are defined according to the impact and scope of each incident. Huawei Cloud will respond to and resolve the incident within a specified time limit according to the priority of the incident, to minimize the impact of the incident on cloud service customers	Customers should classify cybersecurity incidents according to the impact and scope of each incident.
f	the timely handling of cyber security incidents, recording and monitoring progress.	Huawei Cloud has established an incident handling process and complies with the incident response process when a security incident occurs. (Identification, assessment, decision making, and execution of emergency response processing). Huawei Cloud will respond to and resolve the incident within a specified time limit according to the priority of the incident, to minimize the impact of the incident on cloud service customers. Also, Huawei Cloud uses a professional security incident management system to record and track the progress, handling measures, and implementation of all information security incidents, analyze the impact of incident handling.	Customers should ensure the timely handling of cyber security incidents, recording and monitoring progress.

g	the protection of relevant evidence and loggings.	Huawei Cloud has developed security incident emergency handling process and response process. When a server or application is suspected to be intruded, security responders collect evidence for analysis. 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. Moreover, Huawei Cloud reviews the high-risk incident handling process every year to ensure that the high-risk incident handling process meets the company's actual business requirements.	Customers should ensure the protection of relevant evidence and loggings.

h	post-incident activities, such as forensics, root-cause analysis of the incidents.	Huawei Cloud has developed security incident emergency handling process and response process. When a server or application is suspected to be intruded, security responders collect evidence for analysis. 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. Moreover, Huawei Cloud reviews the high-risk incident handling process every year to ensure that the high-risk incident handling process meets the company's actual business requirements. Additionally, Huawei Cloud uses a professional security incident management system to record and track the progress, handling measures, and implementation of all information security incidents, analyze the impact of incident handling, and track and close security incidents in an end-to-end manner to ensure that the entire handling process can be traced, and generate incident reports to summarize lessons learned. The incident reports include a description of the event, the cause, impact, measures taken by Huawei Cloud. Huawei Cloud reviews the high-risk incident handling process every year to ensure that the high-risk incident handling process meets the company's actual business requirements.	Customers should use the knowledge gained in analyzing and resolving information security incidents to reduce the likelihood and impact of future incidents.

i	reporting of suggested improvements to the CISO and the Committee.	Huawei Cloud reviews and summarizes the impact and handling processes of security incidents, and informs and reports to the corresponding affected users and regulatory departments as required. Huawei Cloud has developed a complete process for incident management and notification. If an incident occurs on the Huawei Cloud Base Platform, relevant personnel will analyze the impact of the incident according to the process. If the incident has or will have an impact on the cloud service customers, Huawei Cloud will start to notify customers of the incident. The contents of the notice include but are not limited to description of the incident, the cause, impact, measures taken by Huawei Cloud, and measures recommended for customers. To assist customers in meeting the requirements of cybersecurity incidents reporting to CISO, 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.	When a cybersecurity incident occurs, customers should report to CISO in accordance with this regulation.

j	establish a cyber security incident repository.	Huawei Cloud has established a unified incidents analysis and processing platform to collect, track, and manage security incidents in a unified manner, ensuring that security incidents can be handled and rectified in a timely manner. At the same time, this system records and tracks the progress, handling measures, and implementation of all information security incidents, analyzes the impact of incident handling, and tracks and close security incidents in an end-to-end manner to ensure that the entire handling process can be traced.	Customers should establish a cybersecurity incident repository.

5.3.14 Threat Management

Fully understand the threat landscape of financial institutions.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The threat intelligence management process should be defined, approved and implemented.	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.	Customers should define the threat intelligence management process.
2	The effectiveness of the threat intelligence management process should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established threat intelligence management standards and procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should periodically review and update security requirements for cybersecurity incidents and threats.
3	The threat intelligence management process should include:		

a	the use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tooling, Security Information and Event Monitoring (SIEM), support functions (e.g., Legal, Audit, IT Helpdesk, Forensics, Fraud Management, Risk Management, Compliance);	Huawei Cloud employs its situation awareness (SA) analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. SA incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks. In addition, the system performs real-time evaluation of the security posture of Huawei Cloud, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping Huawei Cloud take necessary security precautions. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The system continuously and analyzes security events in time to detect events and to support cybersecurity event backtracking.	Customers should use dedicated tools (e.g., security intelligence tools) to improve incident detection methods and continuously collect, monitor, and analyze security events. 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 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.
b	the use of reliable and relevant external sources, such as SAMA, government agencies, security forums, (security) vendors, security organizations and specialist notification services;	Huawei PSIRT closely monitors industry-reputable vulnerability databases, security forums, email distribution lists, industry security conferences and other channels to identify Huawei and Huawei Cloud-related vulnerabilities close to real time. Huawei Cloud employs its situation awareness (SA) analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. SA incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks. In addition, the system performs real-time evaluation of the security posture of Huawei Cloud, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping Huawei Cloud take necessary security precautions.	Customers should use the reliable and relevant external sources to collect threat intelligence feeds.

c、d、e	c. a defined methodology to analyze the threat information periodically; d. the relevant details on identified or collected threats, such as modus operandi, actors, motivation and type of threats; e. the relevance of the derived intelligence and the action-ability for follow-up (for e.g., SOC, Risk Management);	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. In addition, Huawei Cloud uses a professional security incident management system to record and track the progress, handling measures, and implementation of all information security incidents, analyze the impact of incident handling, and track and close security incidents in an end-to-end manner to ensure that the entire handling process can be traced.	Customers should use the necessary technology to collect and analyze threat information. And the relevance of the derived intelligence and the action-ability for follow-up should be clarified.

f	f. sharing the relevant intelligence with the relevant stakeholders (e.g., SAMA, BCIS members).	To support the customer's requirement to share threat intelligence with stakeholders, Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services.	Customers should share the relevant intelligence with the relevant stakeholders

5.3.15 Vulnerability Management

To ensure timely identification and effective mitigation of application and infrastructure vulnerabilities in order to reduce the likelihood and business impact for the financial institution.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The vulnerability management process should be defined, approved and implemented.	Huawei Cloud has established a security vulnerability management process, which standardizes the closed-loop process of warning, assessment, and fixing of security vulnerabilities in Huawei Cloud systems. It also requires regular critical security patches to reduce vulnerability risks and specifies the requirements of vulnerabilities classification, responsibilities allocation, and vulnerability handling. Additionally, Huawei Cloud has established a dedicated vulnerability response team to timely evaluate and analyze the causes and threats of vulnerabilities and to formulate remedial measures, to evaluate the feasibility and effectiveness of remedial measures.	Customers should establish effective vulnerability management mechanisms and conduct vulnerability identification and risk assessment for all technology assets.

2	The effectiveness of the vulnerability management process should be measured and periodically evaluated.	Huawei Cloud reviews and updates the established vulnerability management standards and procedures annually. Additionally, Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update the cybersecurity requirements for vulnerability management periodically based on the frequency of the plan.
3	The vulnerability management process should include:		

a	all information assets.	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.	The customer should perform vulnerability scanning on all information assets. 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 security service (CGS – Container Guard Service) that can scan vulnerabilities and configuration information in images, helping enterprises resolve container environment problems that cannot be detected by traditional security software.

b	frequency of performing the vulnerability scan (risk-based).	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. For vulnerabilities that may affect customer service, Huawei Cloud will disclose the vulnerabilities to customers by the Saudi Arabia business service support team, including vulnerability details, vulnerability principle analysis, vulnerability impact scope, vulnerability prevention measures, and vulnerability resolution methods.	Customers scan their information systems for vulnerabilities at a frequency defined by the organization in accordance with the vulnerability scanning process.

c、d、e	c. classification of vulnerabilities. d. defined timelines to mitigate (per classification). e. prioritization for classified information assets.	Huawei Cloud has set up an end-to-end vulnerability response work order system covering every step of the process, and uses the industry best practice Common Vulnerability Scoring System (CVSS) to assess the severity of vulnerabilities, and determines the handling priorities based on the rating of vulnerability exploitation risks on Huawei Cloud, formulates and implements vulnerability remediation plans or avoidance measures，in this way, the SLA requirements for fixing vulnerabilities are specified. In the case of a major vulnerability, the security O&M team uses in-house tools to scan Huawei Cloud network, maps out the scope of affected services, systems and components within minutes. In addition, the security O&M team takes necessary vulnerability mitigation measures based on production environment situation, for example, restricting port access and implementing WAF vulnerability rules to protect or isolate affected services, reducing the risk of vulnerability exploitation. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on tenant services. In addition, Huawei Cloud continuously updates operating system and container images, and rectifies system vulnerabilities by rolling upgrade of the images and containers. This does not affect tenant services.	Customers should analyze the impact of vulnerabilities on critical information assets and determine risk levels and remediation priorities based on their importance.

f	patch management and method of deployment.	Huawei Cloud has established a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. At the same time, Huawei Cloud has formatted a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services. Huawei Cloud implements measures that not only continuously improve cloud products' default security settings, but also front-load security patching to the development phase and simplify security patch deployment.	Customers should establish an effective patch and vulnerability management mechanism, conduct vulnerability identification and risk assessment for all technology assets, test critical patches, and develop a patch update period and patch remediation workflow. Huawei Cloud Image Management Service (IMS) provides simple and convenient self-service management functions for images. Customers can manage their images through the IMS API or the management console. Huawei Cloud staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to refer in deployment testing, troubleshooting, and other O&M activities.

5.4 Third Party Cyber Security

"SAMA Cyber Security Framework" 3.4 "Third Party Cyber Security" requires customers to ensure the same level of cyber security protection is implements at the third party, as within the organization. And provides guidelines for customers to implement business outsourcing. Control requirements for customers cover areas such as service provider capabilities, contracts and agreements and confidentiality of customer data. The relevant control requirements and practices of Huawei Cloud are as follows:

5.4.1 Contract and Vendor Management

To ensure that the financial institution’s approved cyber security requirements are appropriately addressed before signing the contract, and the compliance with the cyber security requirements is being monitored and evaluated during the contract life-cycle.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security requirements should be defined, approved, implemented and communicated within the contract and vendor management processes.	The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. At the same time, Huawei Cloud has also developed a negotiable offline contract template to address specific customer needs.	The contract between the customer and its service provider must clearly specify the service content and level provided, and the cybersecurity responsibilities and obligations of the service provider under the contract.
2	The compliance with contract and vendor management process should be monitored.	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.	Customers should regularly assess compliance with contract and vendor management process, and vendor performance of service contracts.

3	The effectiveness of the cyber security controls within the contract and vendor management process should be measured and periodically evaluated.	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.	Customers should regularly assess the effectiveness of cybersecurity controls within contract and vendor management process.
4	These contract and vendor management processes should cover: a. whether the involvement of the cyber security function is actively required (e.g., in case of due diligence). b. the baseline cyber security requirements which should be applied in all cases. c. the right to periodically perform cyber security reviews and audits.	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.	Customers should require the involvement of cyber security functions in developing contract and vendor management processes, consider applicable cyber security baseline requirements, and conduct regular cyber security reviews and audits.
5	The contract management process should cover requirements for:		

a, b, c, d	a. executing a cyber security risk assessment as part of the procurement process. b. defining the specific cyber security requirements as part of the tender process. c. evaluating the replies of potential vendors on the defined cyber security requirements. d. testing of the agreed cyber security requirements (risk-based).	The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. At the same time, Huawei Cloud has also developed a negotiable offline contract template to address specific customer needs. 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.	Customers should specify in the contract signed with the supplier that performing cyber security risk assessment as part of the procurement process, including cyber security requirements as part of the bidding process, evaluating the supplier's response to cyber security requirements, and testing the agreed cyber security requirements based on risks.
e	defining the communication or escalation process in case of cyber security incidents.	Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If customers' subscribed service is significantly changed or discontinued, Huawei Cloud will notify the customer by releasing a notice on the website or by other means. Huawei Cloud has developed a complete process for incident management and notification. If an incident occurs on the Huawei Cloud Base Platform, relevant personnel will analyze the impact of the incident according to the process. If the incident has or will have an impact on the cloud service customers, Huawei Cloud will start to notify customers of the incident.	Customers should specify the communication or escalation process in case of cyber security incidents in the contract signed with the vendor.

f	ensuring cybersecurity requirements are defined for exiting, terminating or renewing the contract (including escrow agreements if applicable).	The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. Once customers agree the deletion, Huawei Cloud deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, Huawei Cloud clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored. The Cloud Data Migration (CDM) service enables data migration among multiple types of data sources, such as databases, data warehouses, and files, and supports data migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to local data center.	The customer should specify cyber security requirements for or exiting, terminating or renewing the contract.
g	defining a mutual confidentiality agreement.	Huawei Cloud strictly adheres to "not accessing customer data without permission" and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. Huawei Cloud strictly conforms to the cyber security principles described in SAMA and at the same time, it will clearly stipulate the responsibility of Huawei Cloud to customers in the case of a breach of confidentiality clauses in contracts signed with customers.	The customer should specify the confidentiality agreement between the customer and the supplier in the contract signed with the customer.

6	The vendor management process (i.e., service level management) should cover requirements for: a. periodic reporting, reviewing and evaluating the contractually agreed cybersecurity requirements (in SLAs).	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.	Customers should regularly review and update the cyber security requirements agreed upon in the contract with the vendor.

5.4.2 Outsourcing

To ensure that the financial institution’s cyber security requirements are appropriately addressed before, during and while exiting outsourcing contracts.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities
1	The cyber security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within financial institution.	The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. At the same time, Huawei Cloud has also developed a negotiable offline contract template to address specific customer needs.	The customer should define, approve, and implement cybersecurity requirements for the outsourcing policy and process.
2	The cyber security requirements regarding the outsourcing policy and process should	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.	Customers should measure and periodically evaluate cybersecurity requirements for the outsourcing policy and process.

3	The outsourcing process should include: a. the approval from SAMA prior to material outsourcing; b. the involvement of the cyber security function; c. compliance with the SAMA circular on outsourcing.	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.	Customers should approval from SAMA prior to material outsourcing and internal cyber security should be involved in the development of their outsourcing policy.

5.4.3 Cloud Computing

To ensure that all functions and staff within the financial institution are aware of the agreed direction and position on hybrid and public cloud services, the required process to apply for hybrid and public cloud services, the risk appetite on hybrid and public cloud services and the specific cyber security requirements for hybrid and public cloud services.

No.	Specific control requirements	Huawei Cloud Response	Customer Responsibilities

1	The cyber security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and implemented and communicated within Member Organization.	The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. At the same time, Huawei Cloud has also developed a negotiable offline contract template to address specific customer needs. As a cloud service provider, Huawei Cloud ensures secure development, configuration, and deployment of cloud technologies and the security of the operation and management of cloud services. According to ISO 27001, ISO27017, ISO27018, SOC, and CSA STAR, Huawei Cloud has built a comprehensive information security management system and formulated the overall information security strategy of Huawei Cloud. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system documents and the key focus areas and objectives of information security.	Customers should establish cybersecurity requirements related to the use of cloud computing services to ensure the security of information and technology assets of organizations hosted on the cloud.

2	The compliance with the cloud computing policy should be monitored.	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. As a cloud service provider, Huawei Cloud reviews and updates the established information security management system annually, and Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update cybersecurity requirements related to the use of cloud computing.
3	The cyber security controls regarding the cloud computing policy and process for hybrid and public cloud services should be periodically measured and evaluated.	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. As a cloud service provider, Huawei Cloud reviews and updates the established information security management system annually, and Huawei Cloud Computing Security & Privacy Office regularly reviews the implementation of policies to ensure that security governance policies, standards, regulations, and specific measures are implemented in the processes of each business domain.	Customers should review and update cybersecurity requirements related to the use of cloud computing.
4	The cloud computing policy for hybrid and public cloud services should address requirements for:		

a	the process for adopting cloud services, including that: 1. a cyber security risk assessment and due diligence on the cloud service provider and its cloud services should be performed; 2. the Member Organization should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider; 3. a contract should be in place, including the cyber security requirements, before using cloud services;	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. As a cloud service provider, Huawei Cloud ensures secure development, configuration, and deployment of cloud technologies and the security of the operation and management of cloud services.	Customer should conduct a risk assessment of the cloud provider and obtain SAMA approval prior to using cloud services, and should include cybersecurity requirements in contracts signed with cloud service providers.
b	data location, including that: 1. in principle only cloud services should be used that are located in Saudi Arabia, or when cloud services are to be used outside Saudi Arabia that the Member Organization should obtain explicit approval from SAMA;	Huawei Cloud data center is deployed in the Kingdom of Saudi Arabia.	Customers shall ensure that the Data Center is located within the Kingdom of Saudi Arabia, or obtain SAMA approval when using the Cloud Services outside the country.

c	data use limitations, including that: 1. the cloud service provider should not use the Member Organization’s data for secondary purposes;	Huawei Cloud strictly adheres to "not accessing customer data without permission" and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. Huawei Cloud strictly conforms to the cyber security principles described in SAMA. HUAWEI CLOUD focuses on providing cloud services for customers and collects and processes personal data for the purposes specified in the Privacy Policy Statement. HUAWEI CLOUD periodically performs privacy impact assessment for products and services involving personal data, to prevent the collection and processing of personal data exceeding the scope required for actual purposes. Huawei Cloud cooperates with customers to exercise supervision over cloud service providers. The online Huawei Cloud Customer Agreement defines cloud service customers and Huawei's security responsibilities, and the Huawei Cloud Service Level Agreement stipulates the service level provided by Huawei Cloud. At the same time, Huawei Cloud has also developed a negotiable offline contract template to address specific customer needs.	Customers shall specify in the contract or agreement with the cloud service provider that the cloud service shall not use the financial institution's data for other purposes.

d	security, including that: 1. the cloud service provider should implement and monitor the cyber security controls as determined in the risk assessment for protecting the confidentiality, integrity and availability of the Member Organization's data;	As a cloud service provider, Huawei Cloud ensures secure development, configuration, and deployment of cloud technologies and the security of the operation and management of cloud services. In addition, Huawei Cloud has established a cybersecurity risk management specification, which specifies the key processes that should be followed in risk management, the scope of risk management, the departments responsible for risk management, and the standards that should be followed in risk management, identify risks from multiple dimensions. Determine the possibility of risks based on the completeness of security policies, security technologies, and security audits.	Customers should specify the cybersecurity requirements that the cloud service provider should comply with.

e	data segregation, including that: 1. the Member Organization's data is logically segregated from other data held by the cloud service provider, including that the cloud service provider should be able to identify the Member Organization's data and at all times should be able to distinguish it from other data.	Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks. In addition, Huawei Cloud provides multi-layer protection measures. For example, access control and border protection technologies are used to implement coordinated protection against external attacks and strictly implement corresponding management and control measures to ensure Huawei Cloud security. Huawei Cloud facilitates data isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer 3. Tenants can control their own virtual network construction and configuration. On the one hand, a tenant's VPC can be connected to the tenant's enterprise network traditional data center using VPN or Direct Connect service such that tenant's applications and data residing in its internal network can be seamlessly migrated to the tenant's VPC. On the other hand, VPCs are used to build a private network. Then customers can divide the network by planning subnets and configuring routing policies and place storage resources on an internal subnet. In this way, customers can strictly control the ingress and egress	Customers should ensure that the organization's data is logically isolated from other data held by cloud service providers.

		traffic of the subnet and VMs by configuring the network ACLs and relevant rules.	
f	business continuity, including that: 1. business continuity requirements are met in accordance with the Member Organization's business continuity policy;	If a financial institution needs HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. Huawei Cloud established a business continuity management system, to standard business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. Huawei Cloud has obtained the certification of the ISO22301 business continuity management system standard, formulated a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP.	Customers should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure their key businesses.

g	audit, review and monitoring, including that: 1. the Member Organization has the right to perform a cyber security review at the cloud service provider; 2. the Member Organization has the right to perform a cyber security audit at the cloud service provider; 3. the Member Organization has the right to perform a cyber security examination at the cloud service provider;	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.	Customers should conduct cybersecurity reviews, audits, and examination of cloud service providers.

h	exit, including that: 1. the Member Organization has termination rights; 2. the cloud service provider has to return the Member Organization's data on termination; 3. the cloud service provider has to irreversibly delete the Member Organization's data on termination.	When the service agreement terminates, customers can migrate content data from Huawei Cloud through Cloud Data Migration (CDM) service provided by Huawei Cloud, such as migrating to local data center. Once customers agree the deletion, Huawei Cloud deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, Huawei Cloud clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.	Customers should specify in the non-disclosure clauses signed with the third party that secure removal of organization's data by third parties upon end of service. When the service agreement terminates, customers can migrate content data from Huawei Cloud through Cloud Data Migration (CDM) service provided by Huawei Cloud, such as migrating to local data center.

6 Conclusion

This document describes how Huawei Cloud provides cloud services that meet regulatory requirements of the financial industry in the Saudi Arabia and shows that Huawei Cloud complies with key regulatory requirements issued by the Saudi Arabian Monetary Authority（SAMA）. This aims to help customers learn more about Huawei Cloud's compliance with Saudi Arabia '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 document also guides customers on how to design, build, and deploy a secure cloud environment that meets the regulatory requirements of Saudi Arabia's financial industry on Huawei Cloud, and assists customer to better identify security responsibilities together with Huawei Cloud.

This document is for reference only and does not have legal effect or constitute any legal advice. Customers should assess their own use of cloud services as appropriate and ensure compliance with the relevant regulatory requirements from the Saudi Arabia's financial industry when using Huawei Cloud.

7 Version History

Date	Version	Description
2022-7	1.0	First release

