HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in Philippines

Issue 1.1

Date 2024-08-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Overview

1.1 Background and Purpose of Publication

The Republic of the Philippines (hereinafter referred to as the "Philippines") has a diverse history and culture and universal English environment, and is one of the major member states of ASEAN and Asia-Pacific Economic Cooperation (APEC). With the rapid development of information technology and the deepening of China's Belt and Road cooperation in recent years, the Philippine financial industry is facing an increasingly complex environment while flourishing.

Bangko Sentral ng Pilipinas (BSP), the central bank of the Republic of the Philippines, was established on 3 July 1993 as the principal financial services regulator in the Philippines, managing banks and non-bank financial institutions in the Philippines, including quasi-banks, financial companies and non-equity savings and loan associations. BSPs has the financial and administrative autonomy of the national government while performing their statutory duties. The main powers and functions of the BSP are exercised by its Monetary Committee, which has seven members appointed by the President of the Philippines.

Huawei Cloud, as a cloud service provider, is committed not only to helping FIs meet local regulatory requirements, but also to continuously providing them with cloud services and business operating environments meeting FIs' standards. This whitepaper sets out details regarding how Huawei Cloud assists FIs operating in Philippines in meeting regulatory requirements as to the contracting of cloud services.

1.2 Introduction of Applicable Financial Regulatory Requirements in Philippines

Manual of Regulations for Banks(MORB): The Manual of Regulations for Banks (MORB) is designed to be an authoritative regulation governing banks which are all under the supervision of the Bangko Sentral ng Pilipinas. Principally, the MORB fosters compliance to the banking standards and contributes to strengthen the stability of the Philippine financial system.

Manual of Regulations for Non-Bank Financial Institutions(MORNBFI): The Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) is designed to be an authoritative regulation governing non-bank financial institutions (NBFIs) supervised by, or are under the regulatory ambit of, the Bangko Sentral ng Pilipinas (Bangko Sentral).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Circular No. 982, Series of 2017, Enhanced Guidelines on Information Security Management: This guidance is designed to be amending relevant provisions of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) in line with rapidly evolving technology and cyber-threat landscape.

Circular No. 951, Series of 2017, Guidelines on Business Continuity Management: This guidance is designed to be on business continuity management for Bangko Sentral ng Pilipinas (BSP)-supervised financial institutions (BSFIs) and amendments in the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Circular No. 808, Series of 2013, Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions: This guidance is designed to be amendments to Sections X176 and X705 of the Manual of Regulations for Banks (MORB) to enhance the guidelines on information technology risk management.

1.3 Definitions

- **Huawei Cloud**

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

- **Operational risk**

  Operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems; or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Operational risk is inherent in all activities, products and services, and cuts across multiple activities and business lines within the bank and across the different entities in a banking group or conglomerate where the bank belongs.

- **Cloud computing**

  Defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g networks, servers, storage facilities, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- **Cybersecurity** Cybersecurity shall refer to technologies, processes, and practices designed to protect a BSFI's information assets and consumers by preventing, detecting, and responding to cyber-attacks.

- **Information security risk management**

  Information security risk management (ISRM) shall refer to the process of identifying, assessing, mitigating, managing, and monitoring information security risks, including cyber-risks, to ensure these are within acceptable levels. It should be integrated into the BSFI's ISP and enterprise-wide risk management system.

- **Business Continuity**

  Business Continuity shall refer to a state of continued, uninterrupted operation of a business.

- **Board of directors**

  A management body elected by the shareholders to exercise the corporate powers of a locally registered BSI. If it is a BSFI incorporated or incorporated outside the Philippines, it may refer to an institution equivalent to functional oversight, such as a national head (in the case of a foreign bank) or a governing board or an institution authorized to assume supervisory and supervisory responsibilities.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **IT outsourcing**

  IT outsourcing refers to any contractual agreement between a BSFI and a service provider or vendor for the latter to create, maintain, or reengineer the institution's IT architecture, systems and related processes on a continuing basis. A BSFI may outsource IT systems and processes except those functions expressly prohibited by existing regulations. The decision to outsource should fit into the institution's overall strategic plan and corporate objectives and outsourcing arrangement should comply with the provisions of existing Bangko Sentral rules and regulations on outsourcing.

- **Senior management**

  Senior management refers to agency officials authorized by the Board of Directors to carry out policies established by the Board of Directors in the conduct of agency business.

- **Business Continuity Plan (BCP)**

  Business Continuity Plan (BCP) refers to a documented plan detailing the orderly and expeditious process of recovery, resumption, and restoration of business functions in the event of disruptions. It should be able to cover and establish linkages among its multiple components, such as communication plan, crisis management plan, contingency funding plan, and technology recovery plan.

- **Security Operations Center (SOC)**

  A unit or function that provides centralized visibility, continuous monitoring, and rapid response and recovery procedures for security events and events.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Huawei Cloud Certification

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

Huawei Cloud has attained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that Huawei Cloud has achieved internationally recognized best practices in information security management.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC Audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA)

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Certification	Description
	for the system and internal control of outsourced service providers. At present, Huawei Cloud has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that Huawei Cloud has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
CSA STAR Gold Certification	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and cooperation in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. Huawei Cloud FusionSphere passed Common Criteria EAL 3+ certification, indicating that the Huawei Cloud software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that Huawei Cloud has a complete personal data protection management system and is in the global leading position in data security management.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms Huawei Cloud's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that Huawei Cloud operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that Huawei Cloud offers a complete personal data protection system to ensure personal data security.
M&O Certification	Uptime Institute is a globally recognized data center standardization organization and authoritative professional certification organization. Huawei Cloud data center has adopted the world's top data center infrastructure O&M certification (M&O certification) issued by Uptime Institute. The adoption of M&O certification indicates that Huawei Cloud data center O&M

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Certification	Description
	management is at the leading level in the world.
NIST CSF	NIST CSF consists of three parts: the Framework Core, the Implementation Tiers and the Framework Profiles. The Framework Core consists of five concurrent and continuous Functions—Identify Protect Detect Respond Recover. This capability Framework covers the entire cybersecurity process before, during, and after the event, helping enterprises proactively identify, prevent, detect, and respond to security risks.
PCI 3DS Certification	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that Huawei Cloud complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.

Regional standard certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. Huawei Cloud has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key Huawei Cloud regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. Huawei Cloud Singapore has obtained the highest level of MTCS security rating (Level 3).
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that Huawei Cloud services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	Cloud service user data protection capability evaluation is a mechanism for evaluating the security of cloud service user data. Key indicators include pre-event prevention, in-event protection, and post-event tracing.
ITSS Cloud Computing Service Capability Evaluation	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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Certification	Description
by the Ministry of Industry and Information Technology (MIIT) (China)	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.
Trusted Cloud Assessment	Trusted Cloud Assessment is an authoritative evaluation of cloud computing services and products organized by the Data Center Alliance (DCA) and the Telecom Research Institute of the Ministry of Industry and Information Technology (China Academy of Information and Communications Technology (CAICT)).
Cyber Security Review by the Office of Cyber Security	Cyber security review by the Office of Cyber Security is a third-party security review conducted by the Office of the Central Cyberspace Affairs Commission according to the national standard Cloud Computing Service Security Capability Requirements. The HUAWEI CLOUD e-Government cloud platform successfully passed the security review (enhanced level), indicating that the Huawei e-Government cloud platform is recognized by the national cyber security management organization in terms of security and controllability.

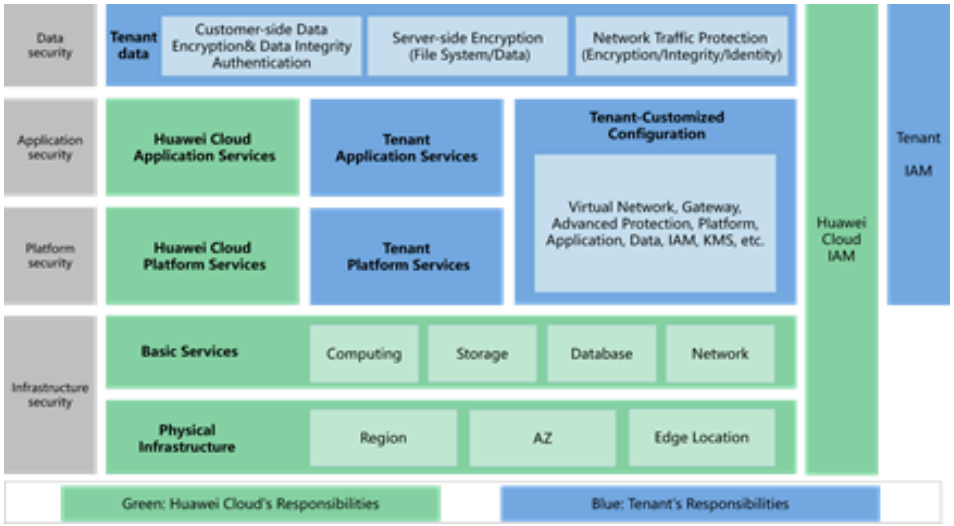
For more information on Huawei Cloud security compliance and downloading relevant compliance certificate, please refer to the official website of Huawei Cloud "Trust Center - Security Compliance".

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Huawei Cloud Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model



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

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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".

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 How Huawei Cloud Complies with and Assists customers to Meet the Requirements of the "Manual of Regulations for Banks" (MORB)

The Manual of Regulations for Banks (MORB) issued by Bangko Sentral ng Pilipinas (BSP) came into effect on December 31, 2018. The Regulation is the primary source of regulations governing entities supervised by Bangko Sentral ng Pilipinas. The regulation imposes requirements on financial institutions primarily from the perspective of IT risk, business continuity, and outsourcing and vendor management managed by banking organizations.

When BSFIs are seeking to comply with the requirements provided in the Manual of Regulations for Banks (MORB), Huawei Cloud, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the Manual of Regulations for Banks (MORB), and explains how Huawei Cloud, as a cloud service provider, can help BSFIs to meet these requirements.

5.1 IT Risk Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Profile Classification	BSFI should perform a higher degree of oversight, due diligence, and risk management controls to outsourcing arrangements. Outsourcing core IT services and functions via cloud computing platforms may further intensify IT and information security risks. Outsourced services.	Customers should conduct due diligence prior to selecting a service provider, particularly in the areas of governance, risk and compliance management. Huawei Cloud will arrange for someone to actively cooperate with the audit and due diligence. Huawei Cloud has obtained ISO 27001, ISO27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System a. IT Governance.	(2) IT Policies, Procedures and Standards. IT policies and procedures should include at least the following areas: 1）IT Governance/Management; 2）Development and Acquisition; 3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating secure and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity.
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System a. IT Governance.	(3) IT audit. BSFI should establish effective audit programs and periodic reporting to the Board on the effectiveness of institution’s IT risk management, internal controls, and IT governance.	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. Huawei Cloud's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			resource tracking, and problem location.
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System c. IT controls implementation.	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1） Information security; 2） Project management/development and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management; 5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers.
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System c. IT controls implementation.	(b) Integrated, holistic and risk-based approach. The ISRM should form an integral part of the BSFI's ISP and enterprise risk management system to manage information security risks to acceptable levels. The ISRM should also consider security controls and requirements over third party service providers, customers, banks, and other third party stakeholders. This is because threat actors may launch their attacks on the BSFI through these third party networks.	Huawei Cloud has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. 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.
148 INFORMATION TECHNOLOGY	IT Risk Management System c. IT	BSFI management should implement an effective outsourcing oversight program that provides the framework for management to understand, monitor,	Customers should establish processes and mechanisms for outsourcing management to ensure that risks related to outsourcing are properly identified and controlled.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
RISK MANAGEMENT	controls implementation.	measure, and control the risks associated with outsourcing. BSFI outsourcing IT services should have a comprehensive outsourcing risk management process which provides guidance on the following areas: 1） risk assessment; 2） selection of service providers; 3） contract review; 4） monitoring of service providers.	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with risk assessment, contract review and other monitoring activities initiated by customers.
148 INFORMATION TECHNOLOGY RISK MANAGEMENT	Reporting and notification standards	a. Reporting requirement. BSFI are required to submit reports to the Bangko Sentral the following reports/information: major Cyber-related Incidents and disruptions of financial services and operations. b. Procedure for event-driven reporting. （1） The BSFI Compliance Officer and/or BSFI-designated Officer shall notify the appropriate supervising department of the Bangko Sentral within two （2） hours from discovery of the reportable major cyber-related incidents and/or disruptions of financial services and operations. （2） The BSFI shall disclose, at the minimum, the nature of the incident and the specific system or business function involved. （3） Within twenty-four (24) hours from the time of the discovery of the reportable major cyber-related incident	Huawei Cloud has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. In addition, Huawei Cloud analyzes the root causes of security incidents and formulates preventive and preventive measures. Huawei Cloud periodically collects statistics on

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and/or disruption, a follow-up report should be sent to the appropriate supervising department of the Bangko Sentral through e-mail indicating the following, as applicable: (a) nature of the incident; (b) manner and time of initial detection; (c) impact of the incident based on initial assessment (e.g., length of downtime, number of affected customers/accounts, number of complaints received, value of transactions involved); (d) initial response or actions taken/to be taken (e.g., conduct of root cause analysis) with respect to the incident; and (e) information if the incident resulted in activation of the Business Continuity Plan (BCP) and/or Crisis Management Plan (CMP). c. Verification of root cause. The BSFI shall perform root cause verification of the reported incident, identify areas for improvement to prevent recurrence of the incident, and subject it to special inspection or supervisory inspection by the Bangko Sentral.	incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.

5.2 Business Continuity Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
149 BUSINESS CONTINUITY MANAGEMENT	Business Continuity Management Plan and Outsourcing	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	Customers should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			services and safeguards customers' service and data security. Huawei Cloud has a disaster recovery 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. In addition, Huawei Cloud has established a crisis communication plan to promptly disclose related incidents and notify customers in accordance, and implement emergency plans and recovery processes to minimize the impact on services in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
149 BUSINESS CONTINUITY MANAGEM	Other policies, standards and processes	Other policies, standards and processes should be integrated into the	Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
ENT		BCM process: a. Pandemic planning. b. Cyber resilience. Cyber-threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated， BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a disaster recovery 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.

5.3 APPENDIX—IT Audit

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
APPENDIX 74 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Audit	5. IT AUDIT PHASES	5.3. Performance of Audit Work. Depending on the complexity of IT risk profile, IT auditors may perform all or a combination of any of the following IT audit procedures: a. IT General Controls Review. The following areas should be covered, among others: a) IT management and strategic planning; b) IT operations; c) Client/server architecture; d) Local and wide-area networks; e) Telecommunications; and f) Physical and information security. b. Application Systems Review - The purpose of this review is to identify, document, test and evaluate the application controls that are implemented to ensure the confidentiality, integrity and accuracy of the system processing and the related data. c. Technical Reviews - BSFI requires IT auditors to perform highly technical/ specialized reviews such as the conduct of periodic internal vulnerability assessment and penetration testing, computer forensics and review of emerging technologies, e.g., cloud computing, virtualization, mobile computing.	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. To meet customers' compliance requirements, Huawei Cloud regularly conducts internal and third-party vulnerability scan, penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. For all known security vulnerabilities, Huawei Cloud evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated. Huawei Cloud organizes internally or external third parties with certain qualifications to conduct penetration tests on all Huawei Cloud systems and applications every six months, and follow up and rectify the results of penetration tests. The penetration test report and follow-up would be verified by internal audits and external certification agencies.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.4 APPENDIX－－Information Security

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.1.1. Risk Management Process. Management should conduct periodic security risk assessment to identify and understand risk on confidentiality, integrity and availability of information and IT systems based on current and detailed knowledge on BSFI’s operating and business environment. This includes identifying information security risks relative to its internal networks, hardware, software, applications, systems interfaces, operations and human elements. The risk assessment should include an identification of information and IT resources to be protected and their potential threats and vulnerabilities. After which, the appropriate risk treatment options (i.e., mitigate, transfer, avoid or accept) should be applied taking into consideration the BSFI's risk appetite and tolerance. Once the BSFI identifies the risks to mitigate, Management can begin to develop risk mitigation strategy. The risk management phases from identification to risk treatment should flow into the BSFI's risk reporting and monitoring activities to ensure effectiveness and continuous improvement of the entire risk	Huawei Cloud has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security, including data protection and classification, data retention and transmission locations, and compliance with laws and regulations for the duration of data retention. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan. The risk assessment report is approved by management upon completion.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		management process.	
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.1.1. Policies, Standards, and Procedures. Management should formulate written information security policies, standards, and procedures which define the institution's control environment and guide employees on the required, expected, and prohibited activities.	Huawei Cloud has established and implemented documented cyber security policies and procedures to provide guidance for cyber security management. The release of cyber security policies and procedures must be approved by managers. Employees can view the released information security policies and procedures as authorized. In addition, Huawei Cloud regularly conducts employee training on corporate policies and culture every year.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.1.1.1. Minimum Baseline Security Standards. Management should put in place minimum baseline security standards (MBSS) to ensure that systems, hardware, and network devices are consistently and securely configured across the organization. Management may refer to leading standards and best practices as well as vendor-specific recommendations in developing their MBSS, taking into consideration the following controls: a. Secure configuration of operating systems, system software, databases, and servers to meet the intended uses with all unnecessary services and programs disabled or removed; b. Periodic checking to ensure that baseline	Huawei Cloud implements a series of network security controls on the physical environment, network, platform, application programming interfaces (APIs), and data to ensure secure infrastructure design and practice. a. Huawei Cloud has established unified baseline configuration standards for server operating systems, system software, database management systems, and network devices that supports service operation by referring to industry best practices to implement unified management of service baseline configurations and specify security configuration requirements for systems/components in the Huawei Cloud production environment, and ensure effective execution and continuous improvement of security configurations.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		standards are consistently complied with; c. Timely deployment of tested and approved patches and security updates; d. Adequate documentation of all configurations and settings of operating systems, system software, databases, and servers; and e. Adequate logging capabilities for all systems, applications, network devices, and databases.	b. The Huawei Cloud O&M team periodically checks and updates system security parameters based on internal security baseline management regulations. Huawei Cloud hardens the security configurations of host operating systems, VMs, databases, and web application components and periodically checks them. c. Huawei Cloud establishes a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. In addition, Huawei Cloud has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services, continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period. d. Security baseline requirements are specified for all configurations and settings of Huawei Cloud OSs, system software, databases, and servers. All products are configured based on the baseline requirements specified in the cyber security redline formulated by Huawei Cloud to ensure that unnecessary functions are restricted.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			e. Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.1.2. Security Training and Awareness Programs. All employees of the organization and, where relevant, contractors and third party users should receive appropriate information security awareness training and regular updates in organizational policies and procedures relevant to their job function. Security training and awareness programs should be designed and tailored to the specific requirements of different groups and stakeholders (i.e., business process/information owners, security specialists, incident responders, etc.).	Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. Huawei Cloud continues security awareness training for employees during their employment. There is a special information security awareness training program for employees. The training frequency for general employees is at least once a year, and the training frequency for core employees is higher. This training includes but is not limited to, on-the-spot speeches and online video courses, information security presentation, and case study.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area:	3. ISP MANAGEMENT	3.3.1.3. Security Screening in Hiring Practices. Management should have a screening procedures, including verification and background checks, should be developed for recruitment of permanent and temporary IT staff,	If permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Simultaneously, to ensure orderly internal

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Information Security		and contractors, particularly for sensitive IT-related jobs or access level. Similar checks should be conducted for all staff, including contractors, at regular intervals throughout their employment, commensurate with the nature and sensitivity of their job functions as well as their access to critical systems. Further, it should establish processes and controls to mitigate risks related to employees' termination/resignation or changing responsibilities.	management and reduce the potential impact of personnel management risks on business continuity and security, Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off-boarding security review.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.1. Technology Design. Management should consider information security and cyber resilience during the infrastructure build-up, systems development and product design. It should ensure that applicable standards and operating procedures are in place for all software, network configurations, and hardware connected to critical systems.	Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. Huawei Cloud and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified, the design engineer will formulate mitigation measures according to the reduction library and the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			security design library and complete the corresponding security design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the security of products and services.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.2. Identity and Access Management. The BSFI should adopt a sound and systematic identity and access management program following the principles of least privilege and segregation of duties. The BSFI should have an effective process to manage user authentication and access control consistent with the criticality and sensitivity of the information/system. The grant, modification, and removal of user access rights should be approved by the information/system owner prior to implementation. Information/system owners or business line managers should ensure that user access rights remain appropriate through a periodic user access re-certification process. Obsolete user accounts or inappropriate access rights should be disabled/removed from	1) Huawei Cloud provides Identity and Access Management (IAM) for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication. IAM provides federation authentication for customers. Customers who have a reliable identity authentication service provider in place can map their federated users to IAM users in a specified period for access to customer's Huawei Cloud resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. Customers should

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		the systems in a timely manner. The BSFI should have password standards in place to ensure that user passwords are not easily compromised (i.e., password syntax, validity, system-enforced password changes). Stronger authentication methods, such as the use of multi-factor authentication techniques, should be deployed for high-risk transactions (e.g., large value funds/wire transfers, enrollment of billers, systems administration functions). Default user accounts defined in new software and hardware should either be disabled or changed and subject to close monitoring. Privileged access and use of emergency IDs should be tightly controlled as it gives the user the ability to override system or application controls.	establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. 2) Huawei Cloud has established Internal operation and maintenance account lifecycle management. It includes account management, account owner/user management, password management, account management monitoring, etc. Once created, new accounts are immediately scoped in for daily O&M by security administrators. All operation and maintenance accounts, accounts of all devices and applications are managed in a unified manner, and are centrally monitored through a unified audit platform, and automatic auditing is performed to ensure the full process management from user creation, authorization, authentication to permission recovery. If the account user wants to use the account, the account administrator can start the authorization process, and authorize by password or by increasing the authority of the account; the applicant and the approver of the account cannot be the same person. Huawei Cloud implements role-based access control and permission management for internal personnel, restricting personnel with different positions and responsibilities to only perform specific operations on authorized targets. Ensure that personnel do not

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			gain unauthorized access through minimal privilege assignment and strict behavioral auditing. 3) 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. 4) O&M: At the same time, when Huawei Cloud O&M personnel access Huawei Cloud Management Network for centralized management of the system, they need to use only identifiable employee identity accounts. In addition, two-factor authentication is used to authenticate cloud personnel, such as USB key, Smart Card and so on. Employee account is used to log on VPN and access gateway to realize the deep audit of user login. Privileged Account Management System binds functional or technical accounts of daily or emergency operations to operation and maintenance teams or individuals. Strong log auditing is supported on the bastion host to ensure that the operation and maintenance personnel's operations on the target host can be located to individuals. Grant privileged or emergency accounts to employees only when necessary for their

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			duties. All applications for privileged or emergency accounts are subject to multiple levels of review and approval.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.2.1. Remote Access. The BSFI, in line with business strategies and needs, may allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as "bring your own device" or BYOD). Management should ensure that such remote access is provided in a safe, secure, and sound manner to manage attendant risks. At a minimum, the BSFI should establish control procedures covering: a. Formal authorization process for granting remote access; b. Risk-based authentication controls for remote access to networks, host data and/or systems, depending on the criticality and sensitivity of information/systems; c. Securing communication channels, access devices and equipment from theft, malware and other threats (i.e., encryption, strong authentication methods, data wipe capabilities, application whitelisting1); and d. Logging and monitoring all remote access communications.	Huawei Cloud employees use unique identity in the internal office network. If the external network needs to be connected to HUAWEI working network, it is necessary to access through VPN. For O&M scenarios, centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. The data center external network operation and maintenance personnel and intranet operation and maintenance personnel centrally manage all local and remote operations of network, server and other equipment, and realize unified access, unified authentication, unified authorization, and unified auditing of equipment resource operation management by users. For remote management of Huawei Cloud, whether from the Internet or office network, it is necessary to first access the resource pool bastion host, and then access related resources from a bastion server.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.3. Network Security. Management should adopt robust and multi-layered controls to prevent and detect unauthorized access, misuse, and other threats from entering and/or spreading into its internal computer networks and systems. Effective controls should be employed to adequately secure system and data within the network which include the following, among others: a. Grouping of network servers, applications, data, and users into security domains or zones (e.g., untrusted external networks, external service providers, or trusted internal networks); b. Adopting security policies for each domain in accordance with the risks, sensitivity of data, user roles, and appropriate access to application systems; c. Establishment of appropriate access requirements within and between each security domain; d. Implementation of appropriate technological controls to meet access requirements consistently; e. Monitoring of cross-domain access for security policy violations and anomalous activity; and f. Maintaining accurate	To simplify network security design, prevent the spread of network attacks on Huawei Cloud, and minimize the impact of attacks, Huawei Cloud divides and isolates security zones and services based on ITUE.408 security zone division principles and best cyber security practices in the industry. Nodes in a security zone have the same security level. Huawei Cloud network architecture design, device selection and configuration, and O&M are considered. Huawei Cloud uses multiple layers of security isolation, access control, and border protection technologies for physical and virtual networks, and strictly implements management and control measures to ensure Huawei Cloud security. Huawei Cloud divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. Huawei Cloud maintains the latest network topology. Huawei Cloud data centers are divided into five key security zones: DMZ, public service, POD-Point of Delivery, OBS-Object-Based Storage, and OM-Operations Management. In addition to the preceding network partitions, Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		network diagrams and data flow charts. Commonly used tools and technologies to secure the network include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and demilitarized zones, among others. As the network complexity as well as threats affecting the network evolve, the BSFI should continuously monitor and enhance its network security and systems to ensure that they remain secure,and resilient.	also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. Huawei Cloud isolates data on the cloud by using the Virtual Private Cloud (VPC). VPC uses the network isolation technology to isolate tenants at Layer 3 networks. Tenants can completely control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using VPNs or Direct Connects, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configure security and access rules on demand to meet tenants' fine-grained network isolation requirements. In terms of network border protection, Huawei Cloud has established a solid and complete border and multi-layer security protection system, and deployed Anti-DDoS, IDS/IPS, and WAF protection mechanisms. Anti-DDoS quickly detects

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			and defends against DDoS attacks and comprehensively defends against traffic attacks and application-layer attacks in real time. WAF detects and defends against web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately. The IDS/IPS detects and blocks network attacks from the Internet in real time and monitors abnormal host behaviors.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.3.1. Virtualization. As BSFIs are increasingly leveraging on virtualization technologies to optimize existing hardware resources, reduce operating expenses and improve IT flexibility and agility to support business needs, additional security risks such as attacks on hypervisor integrity and lack of visibility over intra-host communications and virtual machine (VM) migrations are also rising. To address such risks, Management should extend security policies and standards to apply to virtualized servers and environment. Likewise, it should adopt the following control measures: a. Hypervisor hardening with strict access controls and patch management; b. Inspection of intra-host communications {traffic within VM environments) and	Huawei Cloud adopts a series of security mechanisms for VMs to cope with network security risks. The VM security of Huawei Cloud isolates the network from the platform. On the network layer, a virtual switch provided by the hypervisor on each host is used to configure VLAN, VXLAN, and ACL settings to ensure that the VMs on that host are logically isolated. UVP supports the configuration of security groups to isolate VMs by group. Tenants can create security groups containing multiple VMs to enable those VMs to access each other while maintaining isolation from other VMs. By default, VMs in the same security group can access each other but any two VMs in different security groups cannot access each other. That said, access and communication between any two VMs in different security groups can also be customized by the tenant. Huawei Cloud's professional security team

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		ensuring that security control measures are implemented for confidential/sensitive data stored in VMs; and c. VM creation, provisioning, migration, and changes should undergo proper change management procedures and approval processes similar to deployment of physical network/system devices and servers. The BSFI may also consider implementing next generation firewalls that can restrict access more granularly and prevent virtualization-targeted attacks that exploit known VM vulnerabilities and exploits.	performs security hardening on public images and patches any system vulnerabilities that may occur. Secure, updated public images are created with the help of an image factory and provided to users through Image Management Service (IMS). Pertinent hardening and patch information is also provided to tenants for reference during image testing, troubleshooting, and other O&M activities. When creating VMs, tenants can decide based on their applications and security policies whether to use an up-to-date public image or create a private image that has the required security patches installed.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.3.3.5. Data Security. The BSFI should have information classification strategy guidelines and institute appropriate set of controls and procedures for information protection in accordance with the classification scheme. Information should be protected throughout its life cycle from handling, storage or data-at- rest, transmission or data-in-transit, up to the disposal phase. 3.3.3.5.1. Data-at-Rest. Policies, standards, and procedures as well as risk management controls must be in place to secure the BSFI's information assets, whether stored on	Huawei Cloud uses a series of protection mechanisms to protect tenant data storage security. First, Huawei Cloud provides Key Management Service (KMS). It helps users to centrally manage keys and protect key security. It uses a hardware security module (HSM-Hardware Security Module) to create and manage keys for tenants, preventing the key plaintext from being exposed outside the HSM, thereby preventing key leakage. The services that connect with Huawei Cloud KMS include OBS, cloud hard disk, etc. Secondly, in the encryption scenario where the exclusive encryption meets the higher compliance

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		computer systems, physical media, or in hard- copy documents. The level of protective controls shall depend on the sensitivity and criticality of the information. BSFI should exercise effective oversight over the cloud service provider in terms of adherence to security, performance and uptime, and back-up and recovery arrangements contained in the contract/agreement. 3.3.3.5.1.1. Database security. The BSFI should adopt policies, standards, and procedures to adequately secure databases from unauthorized access, misuse, alteration, leakage and/or tampering. Considering their criticality, sensitivity and business impact, access authorizations to databases should be tightly controlled and monitored. Databases should be configured properly and securely with effective preventive and detective controls such as encryption, integrity checkers, logs and audit trails, among others. 3.3.3.5.2. Data-in-transit. Data transfers are commonly done through physical media or electronic transmission. Policies, standards, and procedures should be in place to keep data secure in physical or electronic	requirements of the tenant, a hardware encryption machine certified by the State Cryptography Administration or FIPS140-2 Level 3 verification is used to perform exclusive encryption for the tenant's business, and the default dual-machine architecture is used to improve reliability. Finally, Huawei Cloud's various storage products such as EVS and VBS provide storage encryption mechanisms. Second, the storage and database services provided by Huawei Cloud are guaranteed to be highly reliable. For example, EVS cloud hard disk uses a multi-copy data redundancy protection mechanism, and adopts measures such as synchronous write and read recovery of copies to ensure data consistency. When hardware failure is detected, it can be automatically repaired in the background, data is quickly and automatically rebuilt, and data durability can reach 99.9999999% . ;OBS object storage service supports the high reliability of object data, and through the high reliability network of business nodes and the multi-redundancy design of nodes, the system design availability reaches 99.995%, which fully meets the high availability requirements of object storage services. Provides multiple redundancy of object data and automatic restoration technology to ensure the data consistency

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		transmission. 3.3.3.5.3. Removal, Transfers and Disposition of Assets. Procedures for the destruction and disposal of media containing sensitive information should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Disposal techniques that the BSFI may implement include deletion, overwriting, degaussing5, destruction of the media. Management should be mindful about residual data being stored in computer-based media as well as dumpster-diving attacks in paper-based information in deciding the best disposal strategy for sensitive information assets.	of multiple objects to provide high reliability of object data. The system design data durability is as high as 99.9999999999%; RDS relational database service adopts hot standby architecture, failure system 1 minute automatic switching. Data is automatically backed up every day, uploaded to the OBS bucket, and the backup files are retained for 732 days. One-click recovery is supported. For database security, Huawei Cloud ensures database security through database security reinforcement and database security design. The database provided by Huawei Cloud has various features to ensure the reliability and security of the tenant database, such as VPC, security group, permission setting, SSL connection, automatic backup, database snapshot, point in time recovery (PITR-Point In Time Recovery), Deploy across Availability Zones and more to protect databases from unauthorized access, misuse, alteration, leaks and/or tampering. At the same time, customers can also use the database security service (DBSS) provided by Huawei Cloud. This service includes two functional modules: database security audit and database security protection. It provides three functions of database audit, data leakage protection, and database firewall, which can comprehensively protect the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			cloud. Database security. For the data in transit, the data from the client to the server and between the server on the Huawei Cloud platform is transmitted through a public information channel. The protection of the data in transit is through virtual private network (VPN) and application layer TLS and certificate management. , Huawei Cloud services provide customers with two access methods: console and API. Both use encrypted transmission protocols to build secure transmission channels, effectively reducing the risk of malicious sniffing of data during network transmission. For data security deletion, after the customer confirms the deletion of data, Huawei Cloud will comprehensively clear the specified data and all its copies. First, delete the index relationship between the customer and the data, and then delete the storage space such as memory and block storage. Perform a clearing operation before reallocation to ensure that the related data and information cannot be restored. When the physical storage medium is scrapped, Huawei Cloud clears the data by degaussing, bending, or breaking the storage medium to ensure that the data on it cannot be recovered.
Appendix 75 IT RISK MANAGEM	3. ISP MANAGEME	3.3.3.7. Encryption. Management should adopt a sound encryption	Huawei Cloud establishes an encryption policy and key management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
ENT STANDARDS AND GUIDELINES Area: Information Security	NT	program covering the following elements: a. Encryption type, level and strength commensurate to the sensitivity of the information based on the institution's data classification policy; b. Effective key management policies and practices to properly safeguard the generation, distribution, storage, entry, use, and archiving of cryptographic keys; and c. Periodic review and testing to ensure that encryption methods deployed still provide the desired level of security vis-a-vis changes in technology and threat landscape.	mechanism for protecting data on technical devices, and specifies the rights and responsibilities of personnel, encryption levels, and encryption methods. For encryption, Huawei Cloud uses the AES encryption method widely used in the industry to encrypt data on the platform. In the scenario where data is transmitted between clients and servers and between servers of the Huawei Cloud via common information channels, data in transit is protected by VPN and TLS and certificate management. Huawei Cloud provides customers with two access modes: console and API. Both use encrypted transmission protocols to construct secure transmission channels. For key management, Huawei Cloud service domains must comply with key management security regulations and implement security control over key generation, key storage, key distribution, key update, and key destruction to prevent key leakage and damage. Huawei Cloud provides the Key Management Service (KMS). Key Management Service (KMS) is a secure, reliable, and easy-to-use key escrow service that facilitates centralized key management in order for users to achieve better key security. The KMS employs Hardware Security Module (HSM) technology for key generation and management, preventing the

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			disclosure of plaintext keys outside HSM.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. ISP MANAGEMENT	3.6.2. Communication Plan. A communication plan for information security incidents should be incorporated in the incident recovery plan to facilitate escalation for appropriate management action and to help manage reputation risk. Incidents that lead to publicly visible disruption to BSFI services should be given utmost attention. Timely notification should be given to all relevant internal and external stakeholders (e.g., employees, customers, vendors, regulators, counterparties, and key service providers, media and the public) following a disruption. Management should consider alternate methods of communication and preparation of predetermined messages tailored to a number of plausible disruption scenarios to ensure various stakeholders are timely, consistently, and effectively informed.	Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	4. CYBER THREAT INTELLIGENCE AND COLLABORATION	4.1.1. Security Operations Center. Centralizing security operations through a security operations center (SOC}, equipped with automated security monitoring tools, defined processes and highly-trained personnel, enables BSFIs to keep pace with the tactics of	Huawei Cloud employs its situation awareness 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. Huawei Cloud can connect to third-party Security

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		advanced threat actors. Considering that it may be difficult for some organizations to establish a mature and fully-operational SOC with the requisite skills, expertise and tools, the BSFI may opt to outsource some or all of its SOC functions to a third party service provider. This may be under a managed security service arrangement either on-premise, off-premise or through cloud computing platforms. In this regard, Management should exercise adequate oversight, due diligence and other risk management controls, and comply with existing Bangko Sentral regulations on outsourcing and cloud computing.	Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components, continuous monitoring and real-time analysis ensure the timely detection of security incidents. Huawei Cloud has developed a security incident management mechanism, including a general security incident response plan and process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents.
Appendix 75 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	4. CYBER THREAT INTELLIGENCE AND COLLABORATION	4.2. Information Sharing and Collaboration. With the stealthier, sophisticated and advanced forms of cyber-threats and attacks confronting the financial services industry, BSFIs should have a collective, coordinated, and strategic response through information sharing and collaboration. Information sharing	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. A corporate-level vulnerability database covering all Huawei products, services and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		allows BSFIs to enhance threat intelligence/ situational awareness that enable quick identification, prevention, and response to emerging and persistent threats. In some cases, BSFIs may need to cooperate with concerned government/regulatory bodies, law enforcement agencies and third party providers to prosecute cyber-criminals, activate government incident response plans or issue warnings/advisories to the public. The extent, breadth, and nature of information sharing activities of BSFIs largely depend on their maturity and capabilities. Moderate to Complex BSFIs should actively engage in information sharing organizations and fora within the financial services industry. At a minimum, BSFIs should define information sharing goals and objectives aligned with their ISSP and ISP. Further, BSFIs should formulate policies and procedures on information sharing activities within and outside their organizations.	solutions, Huawei Cloud included, has been created to ensure the effective logging, tracking, resolution and closure of each and every vulnerability. Huawei Cloud has formulated the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation. Moreover, Huawei Cloud is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies.

5.5 APPENDIX— —Project Management/Development, Acquisition and Change Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 76 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	6. SYSTEM ACQUISITION	6.2. The contract agreement between the BSFI and vendor should be legally binding. The BSFI should ensure all contract agreements outline all expected service levels and are properly executed to protect its interest. It is also important to ensure that vendor technicians and third-party consultants are subjected to at least, or preferably more stringent policies and controls compared to the in-house staff. In the case where contract personnel are employed, written contracts should also be in effect.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. To comply with customer requirements, Huawei Cloud has developed related processes to ensure that services can be provided to customers in a secure and compliant manner. If permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including on-boarding

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			security review, on-the-job security training and enablement, on-boarding qualifications management, and off-boarding security review. The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities.
Appendix 76 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	7. CHANGE MANAGEMENT	7.8. Management should ensure that vendors permitted remote access to network resources are properly authorized. System logs showing activity on the system should be reviewed to ensure that unauthorized remote access has not taken place. Management may institute time of day restrictions for remote access, to limit the duration of time a user can access the network remotely (e.g., only during business hours). Vendors utilizing dial in access should be verified through call back procedures and/or through the use of a modem that can be turned on when authorization has been granted by the system administrator.	Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.

5.6 APPENDIX－－IT Operations

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.1. Environmental Controls. Management should configure the UPS to provide sufficient electricity within milliseconds to power equipment until there is an orderly shutdown or transition to the back-up generator. The back-up generator should generate sufficient power to meet the requirements of mission critical IT and environmental support systems. Similarly, IT operations centers should have independent telecommunication feeds from different vendors. Management should physically secure these cables to avoid accidental or malicious disconnection or severing. In addition, management should document wiring strategies and organize cables with labels or color codes to facilitate easy troubleshooting, repair, and upgrade. Every operations center should have adequate heating, ventilation, and air conditioning （HVAC） systems. Operations centers should be equipped with water detectors under raised flooring to alert management of leaks that may not be readily visible. Management should also consider installing floor drains to prevent water	Huawei Cloud has established comprehensive physical security and environmental security 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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers For physical security, Huawei Cloud imposes further requirements on equipment room location selection, access control, and security measures. When choosing a location for a Huawei Cloud data center, Huawei Cloud factors in the risks of potential natural

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		from collecting beneath raised floors or under valuable computer equipment. A variety of strategies are available for fire suppression. Lastly, Management should consider using video surveillance and recording equipment in all or parts of the facility to monitor activity and deter theft. Management should also use inventory labels, bar codes, and logging procedures to control the inventory of critical and valuable equipment.	disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a Huawei Cloud data center. Site selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water, and telecommunication circuits. 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. Huawei Cloud data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. For environment security, Huawei Cloud has further requirements on electrical security, temperature and humidity control, fire control, routine monitoring, water supply and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			drainage, and Anti-static control. For electrical security, Huawei Cloud data centers employ a multi-level security 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. For 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. For 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. For 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 security hazards and ensures smooth operation of all data center equipment. For 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. For anti-static control: Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			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.
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.3. Change Management& Control. Complex BSFIs should have a change management policy that defines what constitutes a "change" and establishes minimum standards governing the change process. Simple BSFIs may successfully operate with less formality, but should still have written change management policies and procedures.	Huawei Cloud has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of Huawei Cloud Change Committee.
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.4. Patch Management. Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Management should develop a process for managing version control of operating and application software to ensure implementation of the latest releases. Management should also maintain a record of the versions in place and should regularly monitor the Internet and other resources for bulletins about product	Huawei Cloud uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In addition, Huawei Cloud has established a security vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability handling requirements. In addition, Huawei Cloud has established

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		enhancements, security issues, patches or upgrades, or other problems with the current versions of the software.	a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures.
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.6. Network Management Controls. Network standards, design, diagrams and operating procedures should be formally documented, kept updated, communicated to all relevant network staff and reviewed periodically. Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimized by automatic re-routing of communications through alternate routes should critical nodes or links fail. The network should be monitored on a continuous basis to reduce the likelihood of network traffic overload and detect network intrusions. Powerful network analysis and monitoring tools, such as protocol analyzers, network scanning and sniffer tools, are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage （e.g. viewing of unencrypted sensitive information）. The use of network tools should also be tightly restricted to	To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks, which will be covered in more detail throughout the rest of this chapter and the following chapters of the white paper. Huawei Cloud deploys Anti-DDoS devices, IPS devices, and web application firewalls at the network

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		authorized staff only and be subject to stringent approval and review procedures.	boundary to protect the boundary. Anti-DDoS devices can detect DDoS attacks, and IPS has the ability to analyze and block real-time network traffic, and can prevent exceptions. Protocol attacks, brute force attacks, port/vulnerability scanning, virus/Trojan horses, exploits targeting vulnerabilities and other intrusion behaviors. External firewalls can deal with external types of attacks, such as SQL injection, cross-site scripting attacks, and component vulnerabilities. Huawei Cloud strictly protects these border protection tools to prevent unauthorized use.
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.7. Disposal of Media. Management should have procedures for the destruction and disposal of media containing sensitive information. These procedures should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Furthermore, disposal procedures should recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since data can be recovered, additional disposal techniques should be applied to remove sensitive information.	Huawei Cloud uses equipment containing storage media to be managed by a special person, who will format it after use. When the storage medium storing the company's confidential information is scrapped, a special person shall ensure that the information stored on it is cleared and cannot be recovered. The treatment methods include degaussing, physical destruction or low-level formatting. When a physical disk needs to be decommissioned, Huawei Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, Huawei Cloud adheres industry standard practices and keeps a complete data deletion activity log for chain of custody and audit purposes.
Appendix 77	3. IT	3.3.2.9. Event/Problem	Huawei Cloud has developed a

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	OPERATIONS STANDARDS	Management. Management should ensure appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day IT operations. The event/problem management process should be communicated and readily available to all IT operations personnel. Management should ensure it trains all operations personnel to act appropriately during significant events. Employees should also receive training to understand event response escalation procedures.	comprehensive event management process that adheres to the "four fast" principle (e.g. fast discovery, fast demarcation, fast isolation, and fast recovery). Events are responded to systematically according to the impact of the event on customers and the network as a whole. The event is recorded and tracked in the work order system to ensure that the event can be solved as root cause analysis is carried out. The incident management process is communicated to the relevant personnel to ensure that the personnel perform the correct steps when an incident occurs.
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.12. Systems and Data Back-up. The BSFI should ensure that sufficient number of backup copies of essential business information, software and related hardcopy documentations are available for restoration or critical operations. A copy of these information, documentation and software should also be stored in an off-site premise or backup site and any changes should be done periodically and reflected in all copies. The BSFI should back-up and store its data and program files in a secure off-site location to allow restoration of systems, applications, and associated data in the event normal processing is disrupted by a disaster or other significant event. A full system backup should be periodically conducted	User data can be replicated and stored on multiple nodes in Huawei Cloud data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery. Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and should at least consist of the updated version of the operating software, production programs, system utilities and all master and transaction files. The frequency of backup should depend on its criticality, but should be performed after critical modification or updates. Written standards should document back-up methodologies, delineate responsibilities of appropriate personnel, and ensure uniform performance throughout the institution. Management should maintain inventories of back-up media stored off-site and periodically perform physical inventories to ensure all required back-up materials are available. Procedures should include verifying adherence to the back-up schedule and reviewing actual back-up copies for readability. Similarly, management should periodically test back-up copies by actually using them to restore programs and data. All backup media should be properly labeled using standard naming conventions. Management should develop a rotation scheme that addresses varying storage durations as well as transportation and storage of multiple formats of media at the off-site storage location. Transportation to the backup site should be done in controlled and secured manner with proper	services and safeguards customers' service and data security. The Huawei Cloud security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan. When significant changes take place in the organization and environment of Huawei Cloud, the effectiveness of business continuity level would also be tested.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		authorization and record. Procedures for disposal of backup media should also be in place.	
Appendix 77 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.13. Systems Reliability, Availability and Recoverability. ●System Availability BSFIs should achieve high systems availability （or near zero system downtime） for critical systems which is associated with maintaining adequate capacity, reliable performance, fast response time, scalability and swift recovery capability. Built-in redundancies for single points of failure should be developed and contingency plans should be tested so that business and operating disruptions can be minimized. ●Technology Recovery Plan The BSFI should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. In formulating an effective recovery plan, scenario analysis should be included to identify and address various types of contingency scenarios. Scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total inaccessibility of the primary data center should	1) System Availability. Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers" data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance, ensuring business continuity. Huawei Cloud has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		be considered. To strengthen recovery measures relating to large scale disruptions and to achieve risk diversification, rapid operational and backup capabilities at the individual system or application cluster level should be implemented. Recovery and business resumption priorities must be defined accordingly. Specific recovery objectives including recovery time objective（RTO） and recovery point objective（RPO） should be established for systems and applications. ●Alternate sites for technology recovery The BSFI should make arrangements for alternate and recovery sites for their business functions and technology in the event the business premises, key infrastructure and systems supporting critical business functions become unavailable. A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site. ●Disaster Recovery Testing The BSFI should always adopt pre-determined recovery actions that have been tested and endorsed by management. The effectiveness of recovery requirements and the	natural disasters and system failures). 2) Technology Recovery Plan. Huawei Cloud standardizes the emergency response process, formulates an emergency response plan, conducts emergency drills and tests periodically, and continuously optimizes the emergency response mechanism. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP. 3) Alternate sites for technology recovery. Huawei Cloud has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of Huawei Cloud Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		ability of BSFI's personnel in executing or following the necessary emergency and recovery procedures should be tested and validated at least annually. Various scenarios which include total shutdown or inaccessibility of the primary data center, as well as component failure at the individual system or application cluster level should be included in disaster recovery tests. Inter-dependencies between and among critical systems should be included in the tests. BSFIs whose networks and systems are linked to specific service providers and vendors, should consider conducting bilateral or multilateral recovery testing. Business users should be involved in the design and execution of comprehensive test cases so as to obtain assurance that recovered systems function accordingly. The BSFI should also participate in disaster recovery tests of systems hosted overseas. Periodic testing and validation of the recovery capability of backup media should be carried out and assessed for adequacy and effectiveness. Backup tapes and disks containing sensitive data should be encrypted before they are transported offsite for storage.	ensure business continuity on the premise of meeting compliance policies. Huawei Cloud has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. 4) Disaster Recovery Testing. Huawei Cloud develops a business continuity plan and disaster recovery plan and periodically tests them. The Huawei Cloud security drill team regularly develops policies for different product types. (including basic services, operation centers, data centers, and overall organizations) and drills in different scenarios to maintain the effectiveness of the continuity plan.
Appendix 77 IT RISK MANAGEMENT	3. IT OPERATIONS STANDA	3.4.3. Performance Monitoring. The BSFI should implement a process to ensure that the	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
STANDARDS AND GUIDELINES Area: IT Operations	RDS	performance of IT systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. BSFI Management should also conduct performance monitoring for outsourced IT solutions as part of a comprehensive vendor management program. Reports from service providers should include performance metrics, and identify the root causes of problems. Where service providers are subject to SLAs, management should ensure the provider complies with identified action plans, remuneration, or performance penalties.	which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized according to the needs of different customers. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation. In addition, Huawei Cloud will provide dedicated personnel to actively cooperate with customers' monitoring and audit requirements on Huawei Cloud and provide performance reports required by customers. Huawei Cloud provides the CES. Cloud Eye Service (CES) is a comprehensive monitoring platform for Elastic Cloud Servers, bandwidth, and other resources. CES monitors alarms, notifications, and custom reports and diagrams in real time, giving the user a precise understanding of the status of service resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.

5.7 APPENDIX— —IT Outsourcing/Vendor Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 78 IT RISK MANAGEMENT	3. IT OUTSOURCING / VENDOR	3.1 Risk Assessment. Prior to entering into an outsourcing plan, the BSFI should clearly	Customers should conduct risk assessments on their outsourced businesses and preferred service providers

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	RISK MANAGEMENT PROGRAM	define the business requirements for the functions or activities to be outsourced, assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced, the capability of the technology service provider （TSP） and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSFI.	to identify potential risks. Huawei Cloud can cooperate and actively respond to customer needs. In addition, Huawei Cloud has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. Huawei Cloud has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation to manage the supplier's compliance with the specific requirements and contract obligations of Huawei Cloud.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.2 Service Provider Selection. Before selecting a service provider, the BSFI should perform appropriate due diligence of the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity in relation to the services to be outsourced.	Customers should conduct due diligence prior to selecting a service provider, particularly with regard to governance, risk and compliance management mechanisms, to ensure the reliability and security of their service provider. In addition, Huawei Cloud will assign dedicated personnel to actively cooperate with the audit requirements and due diligence initiated by the customer and provide related materials to ensure that the service provider meets Huawei Cloud requirements. 1) Financial soundness. Huawei Cloud is Huawei's service brand. Since its launch in 2017, Huawei Cloud has been developing rapidly and its revenue has

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			maintained a strong growth trend. 2). Reputation. As always, Huawei Cloud adheres to the customer-centric principle, making more and more customers choose Huawei Cloud. Huawei Cloud has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, Huawei Cloud was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. 3). Managerial skills. Huawei Cloud inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, Huawei Cloud can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. 4). Technical capabilities. Huawei Cloud provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. Huawei Cloud has five core

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), Huawei Cloud AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, Huawei Cloud has created a new multi-computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. 5). Operational capability and capacity. Huawei Cloud follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. Huawei Cloud regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
Appendix 78 IT RISK MANAGEMENT	3. IT OUTSOURCING / VENDOR	3.3 Outsourcing Contracts The contract is the legally	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	RISK MANAGEMENT PROGRAM	binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting. The BSFI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services. Agreements should have clauses setting out the rules and limitations on subcontracting. To provide accountability, it may be beneficial for the BSFI to include a provision specifying that the contracting service provider shall remain fully responsible with respect to parts of the services which were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors. An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies.	Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. In addition, Huawei Cloud has developed its own mechanism for supplier management, conducts strict security management on outsourcers and outsourced personnel, and regularly conducts audits and security assessments on suppliers . Huawei Cloud transfers customers' security requirements in contracts to suppliers to ensure that the products and services provided by suppliers can meet the security requirements of Huawei Cloud customers. Huawei Cloud will notify customers in a timely manner when important suppliers change based on customer requirements.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.4. Service Level Agreement （SLA）. The BSFI should link SLA to the provisions in the contract regarding incentives, penalties and contract cancellation in order to protect themselves in the event the service provider failed to meet the required level of performance. Management should closely monitor the service provider's compliance with key SLA provision on the following aspects, among others: ●Availability and timeliness of services; ●Confidentiality and integrity of data; ●Change control; ●Security standards compliance, including vulnerability and penetration management; ●Business continuity compliance; and ●Help desk support.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5. Ongoing Monitoring 3.5.1. Monitoring Program. As outsourcing relationships and interdependencies increase in materiality and complexity, the BS1 needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and	Customer should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. Huawei Cloud will assign dedicated personnel to actively respond to the requirements of customer and provide related

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		quality of services required by the contract. The program should employ effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity, particularly the following: ●contract/SLA performance; ●material problems encountered by the service provider which may impact the BSFI; ●financial condition and risk profile; and ●business continuity plan, the results of testing thereof and the scope for improving it.	materials. Huawei Cloud has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation to manage the supplier's compliance with the specific requirements and contract obligations of Huawei Cloud.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5.3. General Control Environment of the Service Provider. The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSFI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.	Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. Huawei Cloud provides Identity and Access Management (IAM) for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication and performs access control and rights management for users Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.6 Business Continuity Planning Consideration. The BSFI should integrate the provider's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.	Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of he affected area when compliance policies are met, ensuring service continuity. To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its own business characteristics and has obtained the IS0 22301 certification. Huawei Cloud has a formal business

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			continuity plan (BCP) and DR plan (DRP) as well, and conducts BCP drills and DRP tests periodically to ensure continued operations of Huawei Cloud services in the event of a disaster, and the emergency response plan complies with the current organizational and IT environments, and continuously optimize the emergency response mechanism.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.7 Compliance with Bangko Sentral Regulations. The outsourcing agreement should explicitly provide a clause allowing Bangko Sentral and BSFIs' internal and external auditors to review the operations and controls of the service provider as they relate to the outsourced activity.	The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual situation. Huawei Cloud will comply with the requirements specified in the agreements signed with BSFIs and assign dedicated personnel to actively cooperate with BSFIs and financial transaction entities to supervise and supervise the audit and supervision of Huawei Cloud.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	4. EMERGING OUTSOURCING MODELS	4.4. BSFIs should be fully aware of the unique attributes and risks associated with cloud computing, particularly in the following areas: ●Legal and Regulatory Compliance; ●Governance and Risk Management; ●Due Diligence; ●Vendor Management/Performance and Conformance; ●Security and Privacy; ●Data Ownership and	Before customers outsource services such as data processing, data storage, and cloud computing, they must verify the capabilities of the service provider, including Legal and Regulatory Compliance; Governance and Risk Management; Due Diligence; Vendor Management/Performance and Conformance; Security and Privacy; Data security and Business Continuity Planning. As a cloud service provider, Huawei Cloud has the following aspects: 1) Compliance with

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		Data Location and Retrieval; ●Business Continuity Planning.	applicable laws and regulations: The development of Huawei Cloud business follows Huawei's strategy of "one policy for one country/ region, one policy for one customer", and on the basis of compliance with the security regulations and industry supervision requirements of the country or region where the customer is located. Huawei Cloud not only leverages and adopts excellent security practices from throughout the industry but also complies with all applicable country-, and à□g²ÑnʒäÝ□c²fic security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, Huawei Cloud continues to build and mature in areas such as our security related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to customers. Huawei Cloud will also openly and cooperatively tackle cloud security challenges standing should-to-shoulder with customers and partners as well as relevant governments in order to support the security requirements of customers 2) Governance and risk management. Huawei Cloud inherits Huawei's risk

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, Huawei Cloud can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. 3) Due diligence and vender management. Huawei Cloud has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation to manage the supplier's compliance with the specific requirements and contract obligations of Huawei Cloud. Huawei Cloud will assign dedicated personnel to actively respond to the requirements of customer and provide related materials. Customers should ensure that their selected service providers can provide services in accordance with the contract and SLA. Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of FIs. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. 4) Security and Privacy. Huawei Cloud has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. Huawei Cloud has obtained many authoritative security and privacy protection certificates in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on Huawei Cloud. Requirements for obtaining third-party audit reports can be specified in the agreement signed by the customer based on the actual situation. To meet customers' compliance requirements, Huawei Cloud has established a comprehensive information security and privacy protection management system based on various laws and regulations, regulatory requirements, and international or industry standards, and continuously improved it. In addition, 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. 5) Data security. Data security refers to the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			comprehensive protection of users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. Huawei Cloud attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. Huawei Cloud will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, Huawei Cloud will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. 6) Business continuity planning. Huawei Cloud has obtained the certification of the ISO22301 business continuity management system standard, established a business continuity management system internally, and formulated a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	4. EMERGING OUTSOURCING MODELS	4.5. Adoption of community and hybrid cloud deployment models may also be allowed with prior Bangko Sentral approval, subject to the following: ●Compliance with existing Bangko Sentral rules and regulations on outsourcing;. ●Implementation of more robust risk management systems and controls required for these types of arrangements; ●Bangko Sentral may be allowed to perform onsite validation prior to implementing the cloud computing arrangement/s.	Huawei Cloud will identify relevant regulatory requirements and comply with its rules and regulations on outsourcing. BSFIs should establish a risk assessment framework to regularly assess the security of their technology infrastructure, including risks associated with outsourcing arrangements. Huawei Cloud will cooperate with customers in risk assessment as needed. Huawei Cloud has developed a comprehensive information security risk management mechanism, and periodically conducts risk assessment and compliance review to ensure secure and stable running of Huawei Cloud's cloud environment. Meanwhile, Huawei Cloud will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual situation.
Appendix 78 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing/Vendor Management	5. ROLE OF IT AUDIT	5.1. The BSFI should conduct a regular, comprehensive audit of its service provider relationships.	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. At the same time, Huawei Cloud has established a supplier selection and supervision

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			system, through due diligence before signing the contract and regular evaluation to manage the supplier's compliance with the specific requirements and contract obligations of Huawei Cloud.

6 How Huawei Cloud Complies and Assists Customers to Meet the Requirements of the" Manual of Regulations for Non-Bank Financial Institutions" (MORNBFI)

The Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) issued by Bangko Sentral ng Pilipinas (BSP) came into effect on December 31, 2018. The purpose of this manual is to provide an authoritative codification of the relevant regulations for non-bank financial institutions (NBFIs) that are subject to or within the purview of Bangko Sentral ng Pilipinas. Similar to MORB's structure and requirements, Huawei Cloud's responsibilities lie in the information security domain of electronic services and IT risk management on the basis of responding to the same T&C requirements.

When BSFIs are seeking to comply with the requirements provided in the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), Huawei Cloud, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), and explains how Huawei Cloud, as a cloud service provider, can help BSFIs to meet these requirements.

6.1 Risk Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
147-Q INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) a. IT Governance.	(2) IT Policies, Procedures and Standards. IT policies and procedures should include at least the following areas: 1）IT Governance/Management; 2）Development and Acquisition;	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity.
147-Q INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) c. IT controls implementation.	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1） Information security; 2） Project management/development and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management; 5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers.
147-Q INFOR	IT Risk Managem	(b) Integrated, holistic and risk-based approach. The	Huawei Cloud has developed a complete information security risk

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
MATION TECHNOLOGY RISK MANAGEMENT	ent System (ITRMS) c. IT controls implementation. (1)	ISRM should form an integral part of the BSFI's ISP and enterprise risk management system to manage information security risks to acceptable levels. The ISRM should also consider security controls and requirements over third party service providers, customers, banks, and other third party stakeholders. This is because threat actors may launch their attacks on the BSFI through these third party networks.	management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. 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.
147-Q INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) c. IT controls implementation. (1)	(d) Cyber threat intelligence and collaboration. In response to the growing cyber-threat landscape, BSFIs need to step up their information security posture and resilience beyond their respective networks. Likewise, BSFIs need to enhance situational awareness that would provide a keen sense of the threat landscape. Further, BSFIs need to collaborate with each other, including regulators, law enforcement agencies, and other third party stakeholders for a collective, coordinated, and strategic response through information sharing and collaboration.	Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. 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. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			information, including the cloud, is immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed. In addition, Huawei Cloud is equipped with dedicated personnel to maintain contact and establish contact points with industry bodies, risk and compliance organizations, local authorities and regulators.
147-Q INFORMATION TECHNOLOGY RISK MANAGEMENT	Reporting and notification standards.	a. Reporting requirement. BSFI are required to submit reports to the Bangko Sentral the following reports/information: major Cyber-related Incidents and disruptions of financial services and operations. b. Procedure for event-driven reporting. （1） The BSFI Compliance Officer and/or BSFI-designated Officer shall notify the appropriate supervising department of the Bangko Sentral within two （2） hours from discovery of the reportable major cyber-related incidents and/or disruptions of financial services and operations. （2） The BSFI shall disclose, at the minimum, the nature of the incident and the specific system or business function involved. （3） Within twenty-four (24) hours from the time of the discovery of the reportable major cyber-related incident and/or disruption, a follow-up report should be	Huawei Cloud has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. In addition, Huawei Cloud analyzes the root causes of security incidents and formulates preventive and preventive measures. Huawei Cloud periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		sent to the appropriate supervising department of the Bangko Sentral through e-mail indicating the following, as applicable: (a) nature of the incident; (b) manner and time of initial detection; (c) impact of the incident based on initial assessment (e.g., length of downtime, number of affected customers/accounts, number of complaints received, value of transactions involved); (d) initial response or actions taken/to be taken (e.g., conduct of root cause analysis) with respect to the incident; and (e) information if the incident resulted in activation of the Business Continuity Plan (BCP) and/or Crisis Management Plan (CMP). c. Verification of root cause. The BSFI shall perform root cause verification of the reported incident, identify areas for improvement to prevent recurrence of the incident, and subject it to special inspection or supervisory inspection by the Bangko Sentral.	prevent such incidents from occurring.
148-Q BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework c. Plan development.	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud has a Disaster Recovery 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			annotated and archived for continuous improvement of the DRP. In addition, Huawei Cloud has established a crisis communication plan 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 in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
148-Q BUSINESS CONTINUITY MANAGEMENT	Other policies, standards and processes.	Other policies, standards and processes. The following policies, standards and processes should be integrated into the BCM process: a. Pandemic planning. b. Cyber resilience. Cyber-threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated, BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an	Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud will assign dedicated personnel to work with financial institutions to develop business continuity plans, conduct business continuity publicity and training in the organization every year, and conduct emergency drills and tests regularly to continuously optimize the emergency response mechanism.
142-P INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Profile Classification.	BSFI should perform a higher degree of oversight, due diligence, and risk management controls to outsourcing arrangements. Outsourcing core IT services and functions via cloud computing platforms may further intensify IT and information security risks.	As a cloud service provider, Huawei Cloud will assign dedicated personnel to respond to customers' requirements for supervision, due diligence, and risk assessment. In addition, Huawei Cloud has established a supplier selection and monitoring system. Through due diligence before contract signing and periodic evaluation after contract signing, Huawei Cloud manages the compliance of suppliers' specific requirements and contract obligations to ensure that the products and services provided by suppliers can also meet customers' security requirements.
142-P INFOR	Risk Managem	(2) IT Policies, Procedures and Standards. IT policies	Huawei Cloud has established a comprehensive IT risk system

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
MATION TECHNOLOGY RISK MANAGEMENT（ITRM）	ent System (ITRMS) a. IT Governance.	and procedures should include at least the following areas: 1）IT Governance/Management; 2）Development and Acquisition; 3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity.
142-P INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	Risk Management System (ITRMS) c. IT controls implementation.	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1） Information security; 2） Project management/development and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management;	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	
142-P INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	Risk Management System (ITRMS) c. IT controls implementation. (1)	(b) Integrated, holistic and risk-based approach. The ISRM should form an integral part of the BSFI's ISP and enterprise risk management system to manage information security risks to acceptable levels. The ISRM should also consider security controls and requirements over third party service providers, customers, banks, and other third party stakeholders. This is because threat actors may launch their attacks on the BSFI through these third party networks.	Huawei Cloud has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. 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.
142-P INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	Risk Management System (ITRMS) c. IT controls implementation. (1)	(d) Cyber threat intelligence and collaboration. In response to the growing cyber-threat landscape, BSFIs need to step up their information security posture and resilience beyond their respective networks. Likewise, BSFIs need to enhance situational awareness that would provide a keen sense of the threat landscape as it relates to their IT risk and cyber-risk profiles, operating complexities, and business models. Further, BSFIs need to collaborate with each other, including regulators, law enforcement agencies, and other third party stakeholders for a collective, coordinated, and strategic response through information sharing and	Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		collaboration. Information sharing allows BSFIs to enhance threat intelligence that enables quick identification, prevention and response to emerging and persistent threats.	necessary security precautions. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability information, including the cloud, is immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed. In addition, Huawei Cloud is equipped with dedicated personnel to maintain contact and establish contact points with industry bodies, risk and compliance organizations, local authorities and regulators.
143-P BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework	BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five (5) phases, namely: BIA and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system to standardize the business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. In addition, under the framework of the system, business impact analysis and risk assessment are performed regularly, key activities and dependencies are identified, risk levels are evaluated, and countermeasures are formulated for identified threats that may cause cloud service resource interruption, and business continuity plans and disaster recovery plans are formulated. It will be tested regularly and the test results will be annotated and documented for continuous improvement of the plan. In addition, Huawei Cloud can help customers develop and test business continuity plans based on their needs.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
143-P BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework a. Business impact analysis and risk assessment.	a.. Business impact analysis and risk assessment. A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through work-flow analyses, enterprisewide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies.
143-P BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework b. Strategy formulatio	b. Strategy formulation. Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA should be defined, approved, and tested. (1) Recovery strategy. As	The customer should consider developing a recovery strategy based on the results of the business impact analysis. To help customers meet compliance requirements, Huawei Cloud formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
	n	business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure systems availability and recoverability. Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels.	of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.
143-P BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework c. Plan development.	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business operations. 2. BSFI should include a communication plan for	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud has established a crisis communication plan 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 in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
143-P BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework e. Personnel training and plan development	(1) Training program. A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan. (2) Plan maintenance. Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies. BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure these are updated with proper approval and documentation with respect to any significant changes in the business environment or as a result of audit findings.	To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the ISO22301 certification. Each year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Customer should consider updating the Business Continuity Plan at least annually and considering the availability of copies of the Business Continuity Plan. To help customers meet compliance requirements, Huawei Cloud periodically reviews and updates all system documents every year based on the requirements of the internal business continuity management system. Huawei Cloud maintains the list of contacts to be contacted in case of an emergency. After receiving a personnel change notification, Huawei Cloud updates the list in a timely manner. Multiple copies of business continuity plans, emergency response plans, and disaster recovery operation manuals are kept in electronic and paper format and distributed to appropriate management and other key personnel.
143-P BUSINESS CONTIN	Other policies, standards and	Other policies, standards and processes. The following policies, standards and processes	Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
UITY MANAGEMENT	processes.	should be integrated into the BCM process: a. Pandemic planning. b. Cyber resilience. Cyber threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated， BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud will assign dedicated personnel to work with financial institutions to develop business continuity plans, conduct business continuity publicity and training in the organization every year, and conduct emergency drills and tests regularly to continuously optimize

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			the emergency response mechanism.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT profile classification.	BSFI should perform a higher degree of oversight, due diligence, and risk management controls to outsourcing arrangements. Outsourcing core IT services and functions via cloud computing platforms may further intensify IT and information security risks.	As a cloud service provider, Huawei Cloud will assign dedicated personnel to respond to customers' requirements for supervision, due diligence, and risk assessment. In addition, Huawei Cloud has established a supplier selection and monitoring system. Through due diligence before contract signing and periodic evaluation after contract signing, Huawei Cloud manages the compliance of suppliers' specific requirements and contract obligations to ensure that the products and services provided by suppliers can also meet customers' security requirements.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) a. IT Governance.	(2) IT Policies, Procedures and Standards. IT policies and procedures should include at least the following areas: 1）IT Governance/Management; 2）Development and Acquisition; 3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			development security, supplier management, information security incident management, and business continuity.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) b. Risk identification and assessment.	b. Risk identification and assessment. BSFIs should maintain a risk assessment process that drives response selection and controls implementation. An effective IT assessment process begins with the identification of the current and prospective IT risk exposures arising from the institution's IT environment and related processes. The assessments should identify all information assets, any foreseeable internal and external threats to these assets, the likelihood of the threats, and the adequacy of existing controls to mitigate the identified risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels. Once management understands the institution's IT environment and analyzes the risk, it should rank the risks and prioritize its response.	Huawei Cloud has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security, including data protection and classification, data retention and transmission locations, and compliance with laws and regulations for the duration of data retention. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan. The risk assessment report is approved by management upon completion.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) c. IT controls implementation.	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1） Information security; 2） Project management/development	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management; 5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	cloud services for customers in all walks of life and providing empowerment and escorting services for customers.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) c. IT controls implementation. (1)	(b) Integrated, holistic and risk-based approach. The ISRM should form an integral part of the BSFI's ISP and enterprise risk management system to manage information security risks to acceptable levels. The ISRM should also consider security controls and requirements over third party service providers, customers, banks, and other third party stakeholders. This is because threat actors may launch their attacks on the BSFI through these third party networks.	Huawei Cloud has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. 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.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) c. IT controls implementation. (1)	(d) Cyber threat intelligence and collaboration. In response to the growing cyber-threat landscape, BSFIs need to step up their information security posture and resilience beyond their respective networks. Likewise, BSFIs need to enhance situational awareness that would provide a keen sense of the threat landscape. Further, BSFIs need to collaborate with each other, including regulators, law enforcement agencies, and other third party stakeholders for a	Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. In addition, the system performs real-time

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		collective, coordinated, and strategic response through information sharing and collaboration.	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. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability information, including the cloud, is immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed. In addition, Huawei Cloud is equipped with dedicated personnel to maintain contact and establish contact points with industry bodies, risk and compliance organizations, local authorities and regulators.
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	IT Risk Management System (ITRMS) c. IT controls implementation.	BSFI management should implement an effective outsourcing oversight program that provides the framework for management to understand， monitor，measure， and control the risks associated with outsourcing. BSFIs outsourcing IT services should have a comprehensive outsourcing risk management process which provides guidance on the following areas: 1） risk assessment; 2） selection of service providers; 3） contract review; and 4） monitoring of service providers.	Customers should establish processes and mechanisms for outsourcing management to ensure that risks related to outsourcing are properly identified and controlled. Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
145-S INFORMATION TECHNOLOGY RISK MANAGEMENT（ITRM）	Reporting and notification standards.	a. Reporting requirement. BSFI are required to submit reports to the Bangko Sentral the following reports/information: major Cyber-related Incidents and disruptions of financial services and operations. b. Procedure for event-driven reporting. （1） The BSFI Compliance Officer and/or BSFI-designated Officer shall notify the appropriate supervising department of the Bangko Sentral within two （2） hours from discovery of the reportable major cyber-related incidents and/or disruptions of financial services and operations. （2） The BSFI shall disclose, at the minimum, the nature of the incident and the specific system or business function involved. （3） Within twenty-four (24) hours from the time of the discovery of the reportable major cyber-related incident and/or disruption, a follow-up report should be sent to the appropriate supervising department of the Bangko Sentral through e-mail indicating the following, as applicable: (a) nature of the incident; (b) manner and time of initial detection; (c) impact of the incident based on initial assessment (e.g., length of downtime, number of affected customers/accounts,	Huawei Cloud has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. In addition, Huawei Cloud analyzes the root causes of security incidents and formulates preventive and preventive measures. Huawei Cloud periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		number of complaints received, value of transactions involved); (d) initial response or actions taken/to be taken (e.g., conduct of root cause analysis) with respect to the incident; and (e) information if the incident resulted in activation of the Business Continuity Plan (BCP) and/or Crisis Management Plan (CMP). c. Verification of root cause. The BSFI shall perform root cause verification of the reported incident, identify areas for improvement to prevent recurrence of the incident, and subject it to special inspection or supervisory inspection by the Bangko Sentral.	
146-S BUSINESS CONTINUITY MANAGEMENT 1	Business continuity management framework	BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five (5) phases, namely: BIA and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system to standardize the business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. In addition, under the framework of the system, business impact analysis and risk assessment are performed regularly, key activities and dependencies are identified, risk levels are evaluated, and countermeasures are formulated for identified threats that may cause cloud service resource interruption, and business continuity plans and disaster recovery plans are formulated. It will be tested regularly and the test results will be annotated and documented for continuous improvement of the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			plan. In addition, Huawei Cloud can help customers develop and test business continuity plans based on their needs.
146-S BUSINESS CONTINUITY MANAGEMENT 1	Business continuity management framework a. Business impact analysis and risk assessment.	a. Business impact analysis and risk assessment. A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through work-flow analyses, enterprisewide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies.
146-S BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework	b. Strategy formulation. Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA	The customer should consider developing a recovery strategy based on the results of the business impact analysis. To help customers meet compliance requirements, Huawei Cloud formulates comprehensive recovery policies

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
1	b. Strategy formulation.	should be defined, approved, and tested. (1) Recovery strategy. As business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure systems availability and recoverability. Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels.	for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.
146-S BUSINESS CONTINUITY MANAGEMENT 1	Business continuity management framework c. Plan development.	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud has established a crisis communication plan 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 in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
146-S BUSINESS CONTINUITY MANAGEMENT 1	Business continuity management framework e. Personnel training and plan development	(1) Training program. A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan. (2) Plan maintenance. Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies. BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure these are updated with proper approval and documentation with respect to any significant changes in the business environment or as a result of audit findings.	To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the ISO22301 certification. Each year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Customer should consider updating the Business Continuity Plan at least annually and considering the availability of copies of the Business Continuity Plan. To help customers meet compliance requirements, Huawei Cloud periodically reviews and updates all system documents every year based on the requirements of the internal business continuity management system. Huawei Cloud maintains the list of contacts to be contacted in case of an emergency. After receiving a personnel change notification, Huawei Cloud updates the list in a timely manner. Multiple copies of business continuity plans, emergency response plans, and disaster recovery operation manuals are kept in electronic and paper format and distributed to appropriate management and other key personnel.
146-S	Other	Other policies, standards	Huawei Cloud has developed a

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
BUSINESS CONTINUITY MANAGEMENT 1	policies，standards and processes.	and processes. The following policies, standards and processes should be integrated into the BCM process: a. Pandemic planning. b. Cyber resilience. Cyber threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated， BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud will assign dedicated personnel to work with financial institutions to develop business continuity plans, conduct business continuity publicity and training in the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			organization every year, and conduct emergency drills and tests regularly to continuously optimize the emergency response mechanism.
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Profile Classification.	BSFI should perform a higher degree of oversight, due diligence, and risk management controls to outsourcing arrangements . Outsourcing core IT services and functions via cloud computing platforms may further intensify IT and information security risks.	As a cloud service provider, Huawei Cloud will assign dedicated personnel to respond to customers' requirements for supervision, due diligence, and risk assessment. In addition, Huawei Cloud has established a supplier selection and monitoring system. Through due diligence before contract signing and periodic evaluation after contract signing, Huawei Cloud manages the compliance of suppliers' specific requirements and contract obligations to ensure that the products and services provided by suppliers can also meet customers' security requirements.
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) a. IT Governance.	(2) IT Policies, Procedures and Standards. IT policies and procedures should include at least the following areas: 1）IT Governance/Management; 2）Development and Acquisition; 3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity.
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) b. Risk identification and assessment.	b. Risk identification and assessment. BSFIs should maintain a risk assessment process that drives response selection and controls implementation. An effective IT assessment process begins with the identification of the current and prospective IT risk exposures arising from the institution's IT environment and related processes. The assessments should identify all information assets, any foreseeable internal and external threats to these assets, the likelihood of the threats, and the adequacy of existing controls to mitigate the identified risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels. Once management understands the institution's IT environment and analyzes the risk, it should rank the risks and prioritize its response.	Huawei Cloud has developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security, including data protection and classification, data retention and transmission locations, and compliance with laws and regulations for the duration of data retention. The purpose of risk assessment is to identify threats and vulnerabilities based on business processes and asset management, formally record the assessment and develop a risk handling plan. The risk assessment report is approved by management upon completion.
126-N INFORMATION TECHNOLOGY RISK MANAG	IT Risk Management System (ITRMS) c. IT controls implemen	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy:	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management,

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
EMENT	tation.	1） Information security; 2） Project management/development and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management; 5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers.
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) c.IT controls implementation.(1)	(b) Integrated, holistic and risk-based approach. The ISRM should form an integral part of the BSFI's ISP and enterprise risk management system to manage information security risks to acceptable levels. The ISRM should also consider security controls and requirements over third party service providers, customers, banks, and other third party stakeholders. This is because threat actors may launch their attacks on the BSFI through these third party networks.	Huawei Cloud has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve secure and stable operation of the Huawei Cloud environment. 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.
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	IT Risk Management System (ITRMS) c.IT controls implementation	BSFI management should implement an effective outsourcing oversight program that provides the framework for management to understand， monitor， measure， and control the risks associated with outsourcing. BSFIs outsourcing IT services should have a comprehensive outsourcing risk management process which provides guidance on the following areas: 1）	Customers should establish processes and mechanisms for outsourcing management to ensure that risks related to outsourcing are properly identified and controlled. Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		risk assessment; 2） selection of service providers; 3） contract review; and 4） monitoring of service providers.	
126-N INFORMATION TECHNOLOGY RISK MANAGEMENT	Reporting and notification standards.	a. Reporting requirement. BSFI are required to submit reports to the Bangko Sentral the following reports/information: major Cyber-related Incidents and disruptions of financial services and operations. b. Procedure for event-driven reporting. （1） The BSFI Compliance Officer and/or BSFI-designated Officer shall notify the appropriate supervising department of the Bangko Sentral within two （2） hours from discovery of the reportable major cyber-related incidents and/or disruptions of financial services and operations. （2） The BSFI shall disclose, at the minimum, the nature of the incident and the specific system or business function involved. （3） Within twenty-four (24) hours from the time of the discovery of the reportable major cyber-related incident and/or disruption, a follow-up report should be sent to the appropriate supervising department of the Bangko Sentral through e-mail indicating the following, as applicable: (a) nature of the incident; (b) manner and time of initial detection;	Huawei Cloud has developed a security incident management mechanism and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. To cooperate with customers to meet regulatory requirements, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. In addition, Huawei Cloud analyzes the root causes of security incidents and formulates preventive and preventive measures. Huawei Cloud periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		(c) impact of the incident based on initial assessment (e.g., length of downtime, number of affected customers/accounts, number of complaints received, value of transactions involved); (d) initial response or actions taken/to be taken (e.g., conduct of root cause analysis) with respect to the incident; and (e) information if the incident resulted in activation of the Business Continuity Plan (BCP) and/or Crisis Management Plan (CMP). c. Verification of root cause. The BSFI shall perform root cause verification of the reported incident, identify areas for improvement to prevent recurrence of the incident, and subject it to special inspection or supervisory inspection by the Bangko Sentral.	
127-N BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework	BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five (5) phases, namely: BIA and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system to standardize the business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. In addition, under the framework of the system, business impact analysis and risk assessment are performed regularly, key activities and dependencies are identified, risk levels are evaluated, and countermeasures are formulated for identified threats that may cause cloud service resource interruption, and business continuity plans and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			disaster recovery plans are formulated. It will be tested regularly and the test results will be annotated and documented for continuous improvement of the plan. In addition, Huawei Cloud can help customers develop and test business continuity plans based on their needs.
127-N BUSINESS CONTINUITY MANAGEMENT	c. Business impact analysis and risk assessment.	c. Business impact analysis and risk assessment. A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through work-flow analyses, enterprisewide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies.
127-N BUSINE	d. Strategy	d. Strategy formulation. Recovery and resumption	The customer should consider developing a recovery strategy

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
SS CONTINUITY MANAGEMENT	formulation.	strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA should be defined, approved, and tested. (1) Recovery strategy. As business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure systems availability and recoverability. Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels.	based on the results of the business impact analysis. To help customers meet compliance requirements, Huawei Cloud formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.
127-N BUSINESS CONTINUITY MANAGEMENT	e. Plan development.	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption;	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		（4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud has established a crisis communication plan to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			processes to minimize the impact on services in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
127-N BUSINESS CONTINUITY MANAGEMENT	e. Personnel training and plan development	(1) Training program. A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan. (2) Plan maintenance. Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies. BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure these are updated with proper approval and documentation with respect to any significant changes	To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the ISO22301 certification. Each year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Customer should consider updating the Business Continuity Plan at least annually and considering the availability of copies of the Business Continuity Plan. To help customers meet compliance requirements, Huawei Cloud periodically reviews and updates all system documents every year based on the requirements of the internal business continuity management system. Huawei Cloud maintains the list of contacts to be contacted in case of an emergency. After receiving a personnel change notification, Huawei Cloud updates the list in a timely manner. Multiple copies of business continuity plans, emergency response plans, and disaster recovery operation manuals are kept in electronic and paper

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		in the business environment or as a result of audit findings.	format and distributed to appropriate management and other key personnel.
127-N BUSINESS CONTINUITY MANAGEMENT	Other policies, standards and processes.	Other policies, standards and processes. The following policies, standards and processes should be integrated into the BCM process: a. Pandemic planning. b. Cyber resilience. Cyber threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated， BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the	Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	will assign dedicated personnel to work with financial institutions to develop business continuity plans, conduct business continuity publicity and training in the organization every year, and conduct emergency drills and tests regularly to continuously optimize the emergency response mechanism.
126 - T BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework	BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five (5) phases, namely: BIA and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system to standardize the business continuity management framework, purpose and scope, management objectives, roles, and responsibilities. In addition, under the framework of the system, business impact analysis and risk assessment are performed regularly, key activities and dependencies are identified, risk levels are evaluated, and countermeasures are formulated for identified threats that may cause cloud service resource interruption, and business continuity plans and disaster recovery plans are formulated. It will be tested regularly and the test results will be annotated and documented for continuous improvement of the plan. In addition, Huawei Cloud can help customers develop and test business continuity plans based on their needs.
126 - T BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework a. Business impact analysis and risk assessmen	a. Business impact analysis and risk assessment. A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Based on the requirements of this

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
	t.	interdependencies through work-flow analyses, enterprisewide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.	system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies.
126 - T BUSINESS CONTINUITY MANAGEMENT	Business continuity management framework c. Plan development.	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud has established a crisis communication plan 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 in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.
126 - TBUSINESS CONTINUITY MANAGEMENT	Business continuity management framework e. Personnel training and plan development	(1) Training program. A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan. (2) Plan maintenance. Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies. BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure these are updated with proper approval and documentation with respect to any significant changes in the business environment or as a result of audit findings.	To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the ISO22301 certification. Each year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Customer should consider updating the Business Continuity Plan at least annually and considering the availability of copies of the Business Continuity Plan. To help customers meet compliance requirements, Huawei Cloud periodically reviews and updates all system documents every year based on the requirements of the internal business continuity management system. Huawei Cloud maintains the list of contacts to be contacted in case of an emergency. After receiving a personnel change notification, Huawei Cloud updates the list in a timely manner. Multiple copies of business continuity plans, emergency response plans, and disaster recovery operation manuals are kept in electronic and paper format and distributed to appropriate management and other key personnel.
126 - TBUSINE	Other policies，	Other policies, standards and processes. The	Huawei Cloud has developed a business continuity management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
SS CONTINUITY MANAGEMENT	standards and processes.	following policies, standards and processes should be integrated into the BCM process: a. Pandemic planning. b. Cyber resilience. Cyber threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated， BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. c. Information security. Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. d. Interdependencies. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. e. Liquidity risk management. f. Project management. g. Event/problem management. h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	system that meets its business characteristics and has obtained the IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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. In addition, Huawei Cloud will assign dedicated personnel to work with financial institutions to develop business continuity plans, conduct business continuity publicity and training in the organization every year, and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			conduct emergency drills and tests regularly to continuously optimize the emergency response mechanism.

6.2 Electronic Services and Operations

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
701-Q ELECTRONIC BANKING SERVICES	Documentary requirements.	a. Within thirty （30） calendar days from such launching/enhancement，QBs shall submit to the Bangko Sentral through the appropriate. (1) A discussion on the services to be offered/enhanced, the business objectives for such services and the corresponding procedures, both automated and manual, offered through the electronic services channels; (2) A description or diagram of the configuration of the QB's electronic services system and its capabilities showing: (i) how the electronic services system is linked to other host systems or the network infrastructure in the QB; (ii) how transaction and data flow through the network; (iii) what types of telecommunications channels and remote access capabilities (e.g., direct modem dial-in, internet access, or both) exist; and (iv) what	Huawei Cloud will arrange for someone to actively cooperate with the audit. Huawei Cloud has obtained ISO 27001, ISO27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. In addition, Huawei Cloud will provide a list of software and hardware components, a description of the security policies and procedures manual, a brief description of the contingency and disaster recovery plans for electronic facilities and Latest report on the periodic review of the system.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		security controls/measures are installed; (3) A list of software and hardware components indicating the purpose of the software and hardware in the electronic services infrastructure; (4) A description of the security policies and procedures manual containing: (i) description of the QB's security organization; (ii) definition of responsibilities for designing, implementing, and monitoring information security measures; and (iii) established procedures for evaluating policy compliance, enforcing disciplinary measures and reporting security violations; (5) A brief description of the contingency and disaster recovery plans for electronic facilities and event scenario/ problem management plan/program to resolve or address problems, such as complaints errors and intrusions and the availability of back-up facilities; (6) Copy of contract with the communications carrier, arrangements for any liability arising from breaches in the security of the system or from unauthorized/ fraudulent transactions; (7) Copy of the maintenance agreements with the	

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		software/hardware provider/s; and (8) Latest report on the periodic review of the system（if applicable）	

6.3 APPENDIX－－IT Audit

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-61 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Audit	5. IT AUDIT PHASES	5.3 Performance of Audit Work. Depending on the complexity of IT risk profile, IT auditors may perform all or a combination of any of the following IT audit procedures: a. IT General Controls Review –The following areas should be covered, among others: a) IT management and strategic planning; b) IT operations; c) Client/server architecture; d) Local and wide-area networks; e) Telecommunications; and f) Physical and information security. b. Application Systems Review - The purpose of this review is to identify, document, test and evaluate the application controls. c. Technical Reviews - also require IT auditors to perform highly technical/ specialized reviews such as the conduct of periodic internal vulnerability assessment and penetration testing,	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. To meet customers' compliance requirements, Huawei Cloud regularly conducts internal and third-party vulnerability scan, penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. For all known security vulnerabilities, Huawei Cloud evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated. Huawei Cloud organizes internally or external third parties with certain qualifications to conduct penetration tests on all Huawei Cloud systems and applications every six months, and follow up

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		computer forensics and review of emerging technologies, e.g., cloud computing, virtualization, mobile computing.	and rectify the results of penetration tests. The penetration test report and follow-up would be verified by internal audits and external certification agencies.

6.4 APPENDIX— —Information Security

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	1. INFORMATION SECURITY STANDARDS	BSFIs should establish an IS program to manage the risks identified through their assessment, commensurate with the sensitivity of the information and the complexity of their IT risk profile. Management may consider a variety of policies, procedures, and technical controls and adopt measures that appropriately address identified risks.	Huawei Cloud has built an information security management system based on the requirements of ISO27001, ISO27017, ISO27018, SOC, and CSA STAR, and has formulated the overall information security policies, management methods of information security system documents, and key information security directions and objectives. Huawei Cloud has established information security risk management regulations and developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security. Based on the confidentiality, integrity, and availability of assets and business processes, it identifies Huawei Cloud threats and vulnerabilities and conducts risk ratings. The assessment is formally recorded and a risk disposal plan is formulated.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.2. Physical and Environmental Protection. Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities. The BSFI should fully consider the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of its data centers. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could adversely affect the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and	Huawei Cloud has established comprehensive physical security and environmental security protection measures, strategies, and procedures. Huawei Cloud data centers are located on suitable physical sites, as determined from solid site surveys. 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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator.	
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.3. Security Administration and Monitoring. A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function. Management should employ the "least privilege" principle throughout IT operations.	Huawei Cloud uses Identity and Access Management (IAM) to provide users with enterprise-level user account management, identity authentication, and fine-grained access control for cloud resources. IAM provides multi-factor authentication (MFA) to improve the security of account login and important operations. 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. If the account user wants to use the account, the account administrator can initiate the authorization process and authorize the account by using a password or increasing the account's rights. The applicant and approver of the account cannot be the same person. In addition, 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			When Huawei Cloud O&M personnel access the Huawei Cloud management network to centrally manage the system, they must use a unique identifiable employee account. All user accounts are configured with strong password security policies, and their passwords are periodically changed to prevent brute force password cracking. In addition, two-factor authentication, such as USB key and SmartCard, is used to authenticate Huawei Cloud O&M personnel. Employee accounts are used to log in to VPNs and bastion hosts to implement in-depth audit of user logins.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.4. Authentication and Access Control. Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfill one's duties. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization14 should be allowed to access confidential information and use system resources solely for legitimate purposes. The BSFI should have an effective process to manage user authentication and access control. Appropriate user authentication mechanism commensurate with the	Huawei Cloud employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. Access to cloud services: IAM is used to control users' access and manage their rights. 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. If the account user wants to use the account, the account administrator can initiate the authorization process and authorize the account by using a password or increasing the account's rights. The applicant and approver of the account cannot be the same person. In addition, Huawei Cloud implements role-based access control and permission management for internal personnel. Employees with different positions and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		classification of information to be accessed should be selected. The grant, modification and removal of user access rights should be approved by the information owner prior to implementation. A user access re-certification process should be conducted periodically to ensure that user access rights remain appropriate and obsolete user accounts have been removed from the systems.	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. Huawei Cloud has established a periodic access permission review mechanism to ensure that operation logs are enabled to record access permission addition, change, and deletion operations. Security personnel periodically audit access permission change logs. If an uncleared exit account is found, the security personnel will ask the system administrator to clear it. The privileged account management system binds functional accounts or technical accounts for routine or 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 log in to the tenant console or resource instance only after obtaining the customer's authorization. Strong log audit is supported on bastion hosts to ensure that O&M personnel can locate operations on target hosts.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information	3. INFORMATION SECURITY STANDARDS	3.2.5. System Security. The following control procedures and baseline security requirements should be developed to safeguard operating systems，system software and databases， among others: • Clear definition of a	First, for access control, HUAWEI CLOUD's Identity and Access Management (IAM) provides identity authentication and cloud resource access control for customers. When O&M personnel access the HUAWEI CLOUD management network to centrally manage the system, they need to use employee IDs and two-factor authentication, such as USB

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Security		set of access privilege for different groups of users and access to data and programs is controlled by appropriate methods of identification and authentication of users together with proper authorization; • Secure configuration of operating systems，system software，databases and servers to meet the intended uses with all unnecessary services and programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers; • Periodic checking of the integrity of static data （e.g. system parameters）to detect unauthorized changes; • Clear establishment of responsibilities to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified，assessed， tested and applied to the systems in a timely manner;	keys and SmartCards. Employee accounts are used to log in to VPNs and bastion hosts to implement in-depth audit of user logins. 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. For security configuration, HUAWEI CLOUD hardens the security configurations of host operating systems, VMs, databases, and web application components, and allows customers to select appropriate security configurations based on their service requirements. For example, in terms of host security, the host OS uses Huawei Unified Virtualization Platform (UVP) to manage CPU, memory, and I/O resources in isolation. The host OS has been minimized and service security has been hardened. In terms of VM security, HUAWEI CLOUD provides security configurations such as image hardening, network and platform isolation, IP/MAC spoofing control, and security groups. In addition, HUAWEI CLOUD uses an integrity check mechanism to ensure the integrity of system parameters. For example, at the VM OS layer, HUAWEI CLOUD Image Management Service (IMS) supports image integrity check. When a VM is created based on an image, the system automatically checks the image integrity to ensure that the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		• Adequate documentation of all configurations and settings of operating systems，system software，databases and servers; and • Adequate logging and monitoring of system and user activities to detect irregularities and logs are securely protected from manipulation.	created VM contains complete image content. In addition, a comprehensive change management procedure prevents HUAWEI CLOUD internal O&M personnel from changing system configuration parameters without authorization. In addition, HUAWEI CLOUD establishes a security patch management process for patch management and test environments to ensure that security patches are installed within the time limit specified in IT security standards. In addition, HUAWEI CLOUD has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services. Continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period. Huawei Cloud collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. The logs are kept for more than 180 days, and security measures are taken to prevent log tampering to enable compliance and backtracking of network security events. In addition, CTS provides operational records of cloud service resources for tenants, and many products and services also have log recording functions.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Tenants can independently select log retention time according to their own needs to effectively support analysis of abnormal activities.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.6. Cyber Security. The BSFI must evaluate and implement appropriate controls relative to the complexity of its network. An effective approach to adequately secure system and data within the network involves the following, among others: • Grouping of network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems); • Establishment of appropriate access requirements within and between each security domain; • Implementation of appropriate technological controls to meet access requirements consistently; and • Monitoring of cross-domain access for security policy violations and anomalous activity.	Huawei Cloud divides a data center into multiple security zones based on service functions and network security risks to implement physical and logical control and isolation, improving the self-protection and fault tolerance capabilities of the network against intrusions and moles. There are five key security zones: DMZ, PublicService, POD-Point of Delivery, OBS-Object-BasedStorage, and OM-OperationsManagement. To ensure that tenant services do not affect management operations and that devices, resources, and traffic are not monitored, Huawei Cloud divides the communication plane of its network into tenant data plane, service control plane, platform O&M plane, and baseboard management controller (BMC) based on different service functions, security risk levels, and permissions. Management Controller: management plane and data storage plane to ensure proper and secure distribution of network communication traffic related to different services, facilitating separation of duties. Huawei Cloud isolates data on the cloud by using the Virtual Private Cloud (VPC). VPC uses the network isolation technology to isolate tenants at Layer 3 networks. Tenants can fully control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using VPNs or

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Direct Connects, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configure security and access rules on demand to meet tenants' fine-grained network isolation requirements.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.7. Remote Access. Controls over remote access are required to manage risk brought about by external connections to the BSFI's network and computing resources. In protecting information, the BSFI should establish control procedures covering: • Approval process on user requests; • Authentication controls for remote access to networks, host data and/or systems; • Protection (e.g. against theft and malicious software) of equipment and devices; • Logging and monitoring all remote access communications; and Provision of more stringent security controls (i.e. data encryption, two-factor authentication process).	Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. When O&M personnel access the Huawei Cloud management network to centrally manage the system, they need to use employee IDs and two-factor authentication, such as USB keys and SmartCards. Huawei Cloud administrators must pass two-factor authentication before accessing the management plane through bastion hosts. All operations are logged and sent to the centralized log audit system in a timely manner. Strong log audit is supported on bastion hosts to ensure that O&M personnel can locate operations on target hosts. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			auditing.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.8. Encryption. The BSFI should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include the following,: • Provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and • Adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.	Huawei Cloud formulates and implements 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 restoration, and destruction. 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.
Appendix Q-62 IT RISK	3. INFORMATION	3.2.9. Malicious Code Prevention. The BSFI should provide	Huawei Cloud uses the IPS, WAF, antivirus software, and HIDS host intrusion detection

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	SECURITY STANDARDS	protection against the risk of malicious code by implementing appropriate controls at the host and network level to prevent and detect malicious code, as well as engage in appropriate user education. Procedures and responsibilities should be established to detect, prevent, and recover from attacks. The BSFI should put in place adequate controls, such as: • Prohibiting the download and use of unauthorized files and software, and access to doubtful web sites; • Installation and timely update of anti-virus software provided by reputable vendors; and • Disallowing the download of executable files and mobile codes, especially those with known vulnerabilities (e.g. through the use of corporate firewalls18 and proper configuration of the browser software); and Prompt and regular virus scanning of all computing devices and mobile users' computers, and procedures for recovering from virus infections.	system to manage vulnerabilities of system components and networks. IPS can detect and prevent potential network intrusions. WAF is deployed at the network border to protect application software from external attacks such as SQL injection, CSS, and CSRF. Antivirus software provides antivirus protection and firewalls in Windows systems. The HIDS host-based intrusion detection system protects ECSs and reduces the risk of account theft. It provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page tamper protection.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.10. Personnel Security， The BSFI should have a process to verify job application information on all new employees. Screening procedures，including verification and background checks. Management should obtain signed confidentiality，non-disclosure and authorized use agreements before granting new employees and contractors access to IT systems. All employees of the organization and，where relevant，contractors and third-party users，shall receive appropriate IS awareness training and regular updates in organizational policies and procedures relevant to their job function.	Huawei Cloud has developed policies and processes based on ISO27001. Before hiring an employee, if permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Simultaneously, to ensure orderly internal management and reduce the potential impact of personnel management risks on business continuity and security, Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including onboarding security review, on-thejob security training and enablement, onboarding qualifications management, and off boarding security review. The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities. For external personnel, Huawei Cloud signs a non-disclosure agreement with them and conducts information security training, including information security responsibilities. Huawei Cloud continues security awareness training for employees during their employment. There is a special information security awareness training program for employees. This training includes but is not limited to, on-the-spot speeches and online video courses. Cybersecurity awareness courses are held periodically for employees to continually refresh their cybersecurity knowledge and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			help them understand relevant policies and systems. This way, they will be able to distinguish acceptable from unacceptable behavior, assume the responsibilities they have for any wrongdoing regardless of their intent, and abide by all company rules and legal requirements.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.2.11. Systems Development, Acquisition and Maintenance. A framework should be in place describing the tasks and processes for development or acquisition of new systems, assignment and delineation of responsibilities and accountabilities for system deliverables and project milestones. User functional requirements, systems design and technical specifications and service performance expectations should be adequately documented and approved at appropriate management levels. The BSFI's development, acquisition, and audit policies should include guidelines describing the involvement of internal audit and information security personnel in the development or acquisition activities as a means of independently verifying the adequacy of the control and security requirements as they are developed	Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and implemented. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling should be clearly specified. The information and/or process owners should conform to the security requirements for each new system or system acquisition, accept tests against the requirements, and approve implementation of systems in the production environment. The BSFI should have an effective process to introduce application and system changes into its respective environments. The process should encompass development, implementation, and testing of changes to both internally developed software and acquired software. Weak procedures can corrupt applications and introduce new security vulnerabilities.	
Appendix Q-62 IT RISK MANAGEMENT STANDAR	3. INFORMATION SECURITY STANDAR	3.3.1. Activity Monitoring. The BSFI should gain assurance of the adequacy of its risk mitigation strategy and implementation by	Huawei Cloud employs its situation awareness analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
DS AND GUIDELINES Area: Information Security	DS	monitoring network and host activity to identify policy violations and anomalous behavior. The BSFI's security monitoring should, commensurate with the risk, be able to identify control failures before a security incident occurs, detect an intrusion or other security incident in sufficient time to enable an effective and timely response, and support post-event forensics activities.	ensure rapid and thorough detection of ongoing attacks and forecast potential threats. Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components, continuous monitoring and real-time analysis ensure the timely detection of security incidents.
Appendix Q-62 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Information Security	3. INFORMATION SECURITY STANDARDS	3.3.2. IS Incident Management. The BSFI should establish incident response and reporting procedures to handle IS-related incidents. All employees, contractors and third party users shall be required to note and report any observed or suspected security weaknesses in systems. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Therefore, the BSFI should strictly control and monitor access to log files whether on the host or in a centralized logging facility. Where a follow-up action	Huawei Cloud has developed a security incident management mechanism, including a general security incident response plan and process, and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud has formulated the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		against a person or organization after an IS incident involves legal action， evidence shall be collected，retained，and presented to conform to the rules for evidence laid down in the relevant jurisdiction.	event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation. Huawei Cloud is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies. Huawei Cloud collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. The logs are kept for more than 180 days, and security measures are taken to prevent log tampering to enable compliance and backtracking of network security events. In addition, CTS provides operational records of cloud service resources for tenants, and many products and services also have log recording functions. Tenants can independently select log retention time according to their own needs to effectively support analysis of abnormal activities.

6.5 APPENDIX—Project Management/Development、Acquisition and Change Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development、Acquisition and Change Management	4. PROJECT PLANNING AND INITIATION	4.4. During the development and acquisition of new systems or other major IT projects, project plans should address issues such as — a) business requirements for resumption and recovery alternatives; b) information on back-up and storage; c) hardware and software requirements at recovery locations; d) BCP and documentation maintenance; e) disaster recovery testing; and f) staffing and facilities. Likewise, during maintenance, where there are changes to the operating environment, business continuity considerations should be included in the change control process and implementation phase.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Under the framework of the system, business impact analysis and risk assessment are performed regularly. Huawei Cloud formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. In addition, Huawei Cloud has developed a business continuity plan and disaster recovery plan and periodically tested them. The business continuity plan is designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. The DR plan usually takes the cloud platform infrastructure and cloud services in a geographical location or region offline, simulates a disaster, and then performs system processing and transfer according to the DR plan to verify the service and operation functions of the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			faulty location. The test results are annotated and archived. for continuous improvement of the program. User data can be replicated and stored on multiple nodes in Huawei Cloud data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery. Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs. Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers" data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			ensuring business continuity. Huawei Cloud has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development、Acquisition and Change Management	5. System development	5.3. Programming standards should be designed to address issues such as the selection of programming languages and tools, the layout or format of scripted code, interoperability between systems, and the naming conventions of code routines and program libraries. These will enhance the BSFI's ability to decrease coding defects and increase the security, reliability, and maintainability of application programs.	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.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND	6. System acquisition	6.1. Software package acquisition is an alternative to in-house systems	Customers should conduct due diligence prior to selecting a service provider, particularly with

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
GUIDELINES Area: Project Management/Development、Acquisition and Change Management		development and should be subject to broadly similar controls as the project life cycle. A proper software selection analysis should be conducted to ensure that user and business requirements are met. In particular，the process should involve detailed evaluation of the software package and its supplier（e.g. its financial condition，reputation and technical capabilities）. If financial stability is in doubt，alternatives should be developed to reduce the adverse impact from loss of a vendor's service.	regard to governance, risk and compliance management mechanisms. (1)Financial strength: Huawei Cloud is Huawei's service brand. Since its launch in 2017, Huawei Cloud has been developing rapidly and its revenue has maintained a strong growth trend. (2)Business reputation: As always, Huawei Cloud adheres to the customer-centric principle, making more and more customers choose Huawei Cloud. Huawei Cloud has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, Huawei Cloud was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. (3)Technical ability: Huawei Cloud provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. Huawei Cloud has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), Huawei

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, Huawei Cloud has created a new multicomputing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development， Acquisition and Change Management	6. System acquisition	6.2. The contract agreement between the BSFI and vendor should be legally binding. The BSFI should ensure all contract agreements outline all expected service levels and are properly executed to protect its interest. It is also important to ensure that vendor technicians and third-party consultants are subjected to at least， or preferably more stringent policies and controls compared to the in-house staff. In the case where contract personnel are employed，written contracts should also be in effect.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. To comply with customer requirements, Huawei Cloud has developed related processes to ensure that services can be provided to customers in a secure and compliant manner. If permitted by applicable laws, Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including on-boarding security review, on-the-job security training and enablement, on-boarding qualifications management, and off-boarding security review. The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development， Acquisition and Change Management	7. CHANGE MANAGEMENT	7.1 The change management procedures should be formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement	Huawei Cloud has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of Huawei Cloud Change Committee. Huawei Cloud has

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		is obtained from all related parties. 7.2 The change manage process should include the following: • Classification and prioritization of changes and determination of the impact of changes; • Roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel; • Program version controls and audit trails; • Scheduling, tracking, monitoring and implementation of changes to minimize business disruption; • Process for rolling-back changes to re-instate the original	established formal internal testing and acceptance measures to ensure that only appropriate and authorized changes are released to the production environment. Before the change goes live, 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 goes live 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.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		programs, system configuration or data in the event of production release problems; and • Post implementation verification of the changes made (e.g. by checking the versions of major amendments). 7.3. Requested changes should be screened before acceptance to determine alternate methods of making the changes, the cost of changes and time requirements for programming activity. System analysts should assess the impact and validity of the proposed changes and all critical change requests should be set as priority. 7.4. The actual cause that led to the request for change should be identified and adequately documented. Formal reports on analysis for problems raised and status of change requests (including closed and outstanding) should be reported to senior management on a periodic basis.	

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		7.5. Audit trail of all change requests should be maintained. Programmers' activities should be controlled and monitored, and all jobs assigned should also be closely monitored against target completion dates.	
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development、Acquisition and Change Management	7. CHANGE MANAGEMENT	7.6. To enable unforeseen problems to be addressed in a timely and controlled manner, the BSFI should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data-related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day).	Huawei Cloud has also developed a standardized emergency change management process. If emergency changes affect users, they will communicate with users in advance by announcement, mail, telephone, conference, or other means according to the prescribed time limit. If the emergency changes do not meet the prescribed notice time limit, the changes will be upgraded to Huawei Cloud senior leadership, and users will be notified promptly after the changes are implemented. Emergency changes are recorded. The old version and data of the program are retained before the changes are executed. The changes are guaranteed to proceed smoothly through two-person operation to minimize the impact on the production environment.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		7.7. Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible, if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.	
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development， Acquisition and Change Management	7. CHANGE MANAGEMENT	7.8. Management should ensure that vendors permitted remote access to network resources are properly authorized. System logs showing activity on the system should be reviewed to ensure that unauthorized remote access has not taken place. Management may institute time of day restrictions for remote access， to limit the duration of time a user can access the network	Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		remotely（e.g. only during business hours）	and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	8. SYSTEMS TESTING	8.1. A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separate from the production environment. Production data should not be used in development or acceptance testing unless the data has been desensitized (i.e. not disclosing personal or sensitive information) and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are migrated to the production environment.	All cloud services pass multiple security tests before release, including but not limited to micro service-level functions and interface security tests such as authentication, authorization, and session security in the alpha phase; API and protocol fuzzing type of testing incorporated in the beta phase; and database security validation testing in the gamma phase. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. The Huawei Cloud R&D environment adopts hierarchical management, including physical isolation, logical isolation, access control, and data transmission channel approval and audit. In addition, the production data that is not anonymized is strictly controlled for testing. After the data is used, the data needs to be deleted.
Appendix Q-63 IT RISK MANAGEMENT	8. SYSTEMS	8.2. Sufficient testing is important to ensure that	Huawei Cloud has passed multiple rounds of security tests before releasing all

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	TESTING	design and overall reliability of the application systems are in accordance with original specifications. Tests should be conducted using documented test plans that should encompass all predetermined data or processing problems and business scenarios.	cloud services, including but not limited to microservice-level functions and interface security tests such as authentication, authentication, and session security in the Alpha phase. In the Beta phase, service integration is verified through API and protocol fuzzing tests. Special security tests, such as database security, are performed in the gamma phase. The test cases cover the security requirements identified in the security design phase and penetration test cases from the attacker's perspective. In addition, Huawei Cloud takes customer security requirements and industry standards as check items and develops corresponding security test tools. For example, SecureCat can check the security configurations of mainstream OSs and databases in the industry.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	13. DISPOSAL	13.1. The BSFI may sometimes need to remove surplus or obsolete hardware, software, or data. Primary tasks include the transfer, archiving, or destruction of data records. Management should transfer data from production systems in a planned and controlled manner that includes appropriate backup and testing	During the destruction of customer content data, Huawei Cloud deletes the specified data and all copies of the data. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		procedures. The BSFI should maintain archived repository of data in accordance with applicable record retention requirements and system documentation to facilitate reinstallation of a system into production, when necessary. Management should destroy data by overwriting old information or degaussing (demagnetizing) disks and tapes.	clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.
Appendix Q-63 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Project Management/Development, Acquisition and Change Management	14. ROLE OF AUDIT, INFORMATION SECURITY AND QUALITY ASSURANCE OFFICERS	14.2 Information Security. The BSFI should ensure that systems are developed, acquired and maintained with appropriate security controls. To do this, management should ensure that — a) systems are developed and implemented with necessary security features enabled and based on established security control requirements; b) software is trustworthy by implementing appropriate controls in the different project phases; and c) appropriate configuration management and	For the security of the development process, Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		change control processes exist, including an effective patch management process. Management should establish security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access, damage or other threats.	lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. Huawei Cloud 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. In addition, Huawei Cloud has developed change management regulations and change processes. Different change types must comply with different change management processes. Each change must be reviewed in multiple phases. 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.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			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. Huawei Cloud establishes a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. In addition, Huawei Cloud has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services. Continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period.

6.6 APPENDIX——IT Operations

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix	3. IT	3.1 Technology	Huawei Cloud uses the CAM

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	OPERATIONS STANDARDS	Inventory. BSFI management should perform and maintain an inventory of all its IT resources, recognize interdependencies of these systems and understand how these systems support the associated business lines. Management should ensure the inventory is updated on an on-going basis to reflect the BSFI's IT environment at any point in time.	asset management system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and generate an asset list. Huawei Cloud assigns an owner to each asset. Huawei Cloud has developed 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. Ensure that the company's assets are properly protected and shared.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.2. Risk Assessment. Once inventory is complete, management should employ a variety of risk assessment techniques to identify threats and vulnerabilities to its IT operations	Huawei Cloud has developed information security risk assessment methods to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, and security audits, and periodically perform information security risk assessment as required. Risk assessment covers all aspects of information security. Based on the confidentiality, integrity, and availability of business processes and assets, identify and rate threats and vulnerabilities of Huawei Cloud, formally record the assessment, develop a risk handling plan, and monitor the implementation of the risk handling plan.
Appendix	3. IT	3.3.2.1. Environmental	Huawei Cloud has established

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	OPERATIONS STANDARDS	Controls.. Management should configure the UPS. The back-up generator should generate sufficient power to meet the requirements of mission critical IT and environmental support systems. Similarly， IT operations centers should have independent telecommunication feeds from different vendors. Management should physically secure these cables to avoid accidental or malicious disconnection or severing. Every operations center should have adequate heating， ventilation， and air conditioning （HVAC） systems. Organizations should plan their HVAC systems with the requirements of their IT systems in mind. Operations centers should be equipped with water detectors under raised flooring .Management should also consider installing floor drains to prevent water from collecting beneath raised floors or under valuable computer equipment.A variety of strategies are available for fire suppression. Lastly， Management should consider using video surveillance and recording equipment in all or parts of the facility to monitor activity and deter theft. Management	comprehensive physical security and environmental security 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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers For physical security, Huawei Cloud imposes further requirements on equipment room location selection, access control, and security measures. When choosing a location for a Huawei Cloud data center, Huawei Cloud factors in the risks of potential natural disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a Huawei Cloud data center. Site selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		should also use inventory labels， bar codes， and logging procedures to control the inventory of critical and valuable equipment.	and telecommunication circuits. 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. Huawei Cloud data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. For environment security, Huawei Cloud has further requirements on electrical security, temperature and humidity control, fire control, routine monitoring, water supply and drainage, and Anti-static control. For electrical security, Huawei Cloud data centers employ a multi-level security 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. For 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			optimally within their specified ranges of temperature and humidity. For 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. For 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 security hazards and ensures smooth operation of all data center equipment. For 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. For 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.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.3. Change Management & Control. Complex BSFIs should have a change management policy that defines what constitutes a "change" and establishes minimum standards governing the change process. Simple BSFIs may successfully operate with less formality， but should still have written change	Huawei Cloud has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		management policies and procedures.	impacts. Changes can be released only after achieving the approval of Huawei Cloud Change Committee.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.4. Patch Management. Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Management should develop a process for managing version control of operating and application software to ensure implementation of the latest releases. Management should also maintain a record of the versions in place and should regularly monitor the Internet and other resources for bulletins about product enhancements, security issues, patches or upgrades, or other problems with the current versions of the software.	Huawei Cloud uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In addition, Huawei Cloud has established a security vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability handling requirements. In addition, Huawei Cloud has established a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.6. Network Management Controls. Network standards, design, diagrams and operating procedures should be formally documented, kept updated, communicated to all relevant network staff and reviewed periodically.	To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimized by automatic re-routing of communications through alternate routes should critical nodes or links fail. The network should be monitored on a continuous basis to reduce the likelihood of network traffic overload and detect network intrusions. Powerful network analysis and monitoring tools， such as protocol analyzers，network scanning and sniffer tools， are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage （e.g. viewing of unencrypted sensitive information）. The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.	network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks, which will be covered in more detail throughout the rest of this chapter and the following chapters of the white paper. Huawei Cloud deploys Anti-DDoS devices, IPS devices, and web application firewalls at the network boundary to protect the boundary. Anti-DDoS devices can detect DDoS attacks, and IPS has the ability to analyze and block real-time network traffic, and can prevent exceptions. Protocol attacks, brute force attacks, port/vulnerability scanning, virus/Trojan horses, exploits targeting vulnerabilities and other intrusion behaviors. External firewalls can deal with external types of attacks, such as SQL injection, cross-site scripting attacks, and component vulnerabilities. Huawei Cloud strictly protects these border protection tools to prevent unauthorized use.
Appendix Q-64 IT RISK MANAGEMENT STANDAR	3. IT OPERATIONS STANDARDS	3.3.2.7. Disposal of Media. Management should have procedures for the destruction and disposal of media containing sensitive	Huawei Cloud uses equipment containing storage media to be managed by a special person, who will format it after use. When the storage medium storing the company's confidential

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
DS AND GUIDELINES Area: IT Operations		information. These procedures should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Furthermore, disposal procedures should recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since data can be recovered, additional disposal techniques should be applied to remove sensitive information.	information is scrapped, a special person shall ensure that the information stored on it is cleared and cannot be recovered. The treatment methods include degaussing, physical destruction or low-level formatting. When a physical disk needs to be decommissioned, Huawei Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, Huawei Cloud adheres industry standard practices and keeps a complete data deletion activity log for chain of custody and audit purposes.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.3.2.9. Event/Problem Management. Management should ensure appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day IT operations. The event/problem management process should be communicated and readily available to all IT operations personnel. Management should ensure it trains all operations personnel to act appropriately during significant events. Employees should also receive training to understand event response escalation procedures.	Huawei Cloud has developed a comprehensive event management process that adheres to the "four fast" principle (e.g. fast discovery, fast demarcation, fast isolation, and fast recovery). Events are responded to systematically according to the impact of the event on customers and the network as a whole. The event is recorded and tracked in the work order system to ensure that the event can be solved as root cause analysis is carried out. The incident management process is communicated to the relevant personnel to ensure that the personnel perform the correct steps when an incident occurs.
Appendix	3. IT	3.3.2.12. Systems and	User data can be replicated and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	OPERATIONS STANDARDS	Data Back-up. The BSFI should back-up and store its data and program files in a secure off-site location to allow restoration of systems，applications， Written standards should document back-up methodologies，delineate responsibilities of appropriate personnel，and ensure uniform performance throughout the institution. Management should maintain inventories of back-up media stored off-site and periodically perform physical inventories to ensure all required back up materials are available.	stored on multiple nodes in Huawei Cloud data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery. Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. The Huawei Cloud security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan. When significant changes take place in the organization and environment of Huawei Cloud, the effectiveness of business continuity level would also be tested.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND	3. IT OPERATIONS STANDARDS	3.3.2.13. Systems Reliability，Availability and Recoverability. • System Availability. BSFIs should achieve	1) System Availability. Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers" data center clustering architecture. Data centers are located

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
GUIDELINES Area: IT Operations		high systems availability （or near zero system downtime）for critical systems which is associated with maintaining adequate capacity， reliable performance， fast response time， scalability and swift recovery capability. Built-in redundancies for single points of failure should be developed and contingency plans should be tested so that business and operating disruptions can be minimized. • Technology Recovery Plan. BSFI should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. In formulating an effective recovery plan， scenario analysis should be included to identify and address various types of contingency scenarios. Scenarios such as major system outages which may be caused by system faults， hardware malfunction， operating errors or security incidents as well as a total inaccessibility of the primary data center should be considered. • Alternate sites for technology recovery	throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance, ensuring business continuity. Huawei Cloud has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure. 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). 2) Technology Recovery Plan. Huawei Cloud standardizes the emergency response process, formulates an emergency response plan, conducts emergency drills and tests periodically, and continuously optimizes the emergency response mechanism. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		The BSFI should make arrangements for alternate and recovery sites for their business functions and technology in the event the business premises，key infrastructure and systems supporting critical business functions become unavailable. A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site.The recovery facility should be at a distance that would protect it from damage from any incident occurring at the primary site. • Disaster Recovery Testing. The BSFI should always adopt pre-determined recovery actions that have been tested and endorsed by management. The effectiveness of recovery requirements and the ability of BSFI's personnel in executing or following the necessary emergency and recovery procedures should be tested and validated at least annually. Various scenarios which include total shutdown or inaccessibility of the primary data center， as well as component	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. 3) Alternate sites for technology recovery. Huawei Cloud has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of Huawei Cloud Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. Huawei Cloud has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. 4) Disaster Recovery Testing. Huawei Cloud develops a business continuity plan and disaster recovery plan and periodically tests them. The Huawei Cloud security drill team regularly develops policies for different product types. (including basic services,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		failure at the individual system or application cluster level should be included in disaster recovery tests. Inter-dependencies between and among critical systems should be included in the tests. BSFIs whose networks and systems are linked to specific service providers and vendors，should consider conducting bilateral or multilateral recovery testing.	operation centers, data centers, and overall organizations) and drills in different scenarios to maintain the effectiveness of the continuity plan.
Appendix Q-64 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Operations	3. IT OPERATIONS STANDARDS	3.4.1. Service Level Agreement (SLA). BSFI Management of IT functions should formulate an SLA with business units which will measure the effectiveness and efficiency of delivering IT services.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation.

6.7 APPENDIX— —IT Outsourcing / Vendor Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINE	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.1 Risk Assessment. Prior to entering into an outsourcing plan， the BSFI should clearly define the business requirements for the functions or activities to be outsourced，	Customer should conduct a risk assessment of its outsourced business and its preferred service provider to identify potential risks. Huawei Cloud will assign dedicated personnel to respond to customer requirements and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
S Area: IT Outsourcing / Vendor Management		assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced， the capability of the technology service provider （TSP） and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSFI.	provide related materials. In addition, Huawei Cloud has developed a comprehensive information security risk management mechanism and regularly conducts risk assessment and compliance review to ensure secure and stable running of the Huawei Cloud environment. Huawei Cloud has established a supplier selection and monitoring system to manage suppliers' compliance with Huawei Cloud requirements and contract obligations through due diligence before contract signing and periodic evaluation after contract signing.
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.2 Service Provider Selection. Before selecting a service provider， the BSFI should perform appropriate due diligence of the provider's financial soundness，reputation，managerial skills， technical capabilities，operational capability and capacity in relation to the services to be outsourced.	Customers should conduct due diligence prior to selecting a service provider, particularly with regard to governance, risk and compliance management mechanisms. (1) Financial soundness. Huawei Cloud is Huawei's service brand. Since its launch in 2017, Huawei Cloud has been developing rapidly and its revenue has maintained a strong growth trend. (2). Reputation. As always, Huawei Cloud adheres to the customer-centric principle, making more and more customers choose Huawei Cloud. Huawei Cloud has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. (3). Managerial skills. Huawei Cloud inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, Huawei Cloud can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. (4). Technical capabilities. Huawei Cloud provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. Huawei Cloud has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), Huawei Cloud AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, Huawei Cloud has created a new multi-computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			run at the optimal computing power to maximize customer value. (5). Operational capability. Huawei Cloud follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. Huawei Cloud regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.3 Outsourcing Contracts The contract is the legally binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance，reliability， security，confidentiality and reporting. The BSFI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services. Agreements should have clauses setting out	Huawei Cloud provides the Huawei Cloud User Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level provided by Huawei Cloud, and the customer's audit rights and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of financial institutions. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. Huawei Cloud will also assign dedicated personnel to cooperate with the customer in reviewing the contract and provide relevant

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		the rules and limitations on subcontracting. To provide accountability，it may be beneficial for the BSFI to include a provision specifying that the contracting service provider shall remain fully responsible with respect to parts of the services which were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors. An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies.	materials. Huawei Cloud has established a comprehensive supplier management mechanism. It strictly manages the security of outsourcers and outsourced personnel, and regularly audits and evaluates suppliers' security. Huawei Cloud transfers customers' security requirements in contracts to suppliers to ensure that the products and services provided by suppliers can meet the security requirements of Huawei Cloud customers. In addition, Huawei Cloud will notify customers in a timely manner when important suppliers change based on customer requirements.
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.4. Service Level Agreement（SLA）.SLAs formalize the performance standards against which the quantity and quality of service should be measured. Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations， as well as establish accountability for the outsourced activity. The BSFI should link	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		SLA to the provisions in the contract regarding incentives，penalties and contract cancellation in order to protect themselves in the event the service provider failed to meet the required level of performance. Management should closely monitor the service provider's compliance with key SLA provision on the following aspects，among others: ●Availability and timeliness of services; ●Confidentiality and integrity of data; ●Change control; ●Security standards compliance, including vulnerability and penetration management; ●Business continuity compliance; and ●Help desk support.	
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5.1. Monitoring Program. As outsourcing relationships and interdependencies increase in materiality and complexity， the BS1 needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract.	Financial institutions should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. Huawei Cloud will assign dedicated personnel to actively respond to the requirements of financial institutions and provide related materials. In addition, Huawei Cloud has established a supplier selection and monitoring system to manage suppliers' compliance

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		The program should employ effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity，particularly the following: ●contract/SLA performance; ●material problems encountered by the service provider which may impact the BSFI; ●financial condition and risk profile; and ●business continuity plan， the results of testing thereof and the scope for improving it.	with Huawei Cloud requirements and contract obligations through due diligence before contract signing and periodic evaluation after contract signing.
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5.3. General Control Environment of the Service Provider. The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSFI's systems， and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.	Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. Huawei Cloud provides Identity and Access Management (IAM) for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication and performs access control and rights management for users Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.6 Business Continuity Planning Consideration. The BSFI should integrate the provider's BCP into its own plan，communicate functions to the appropriate personnel， and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.	Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of he affected area when compliance policies are met, ensuring service continuity. To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its own business characteristics and has obtained the IS0 22301 certification. Huawei Cloud has a formal business continuity plan (BCP) and DR plan (DRP) as well, and conducts BCP drills and DRP tests periodically to ensure continued operations of Huawei Cloud services in the event of a disaster, and the emergency response plan complies with the current organizational and IT environments, and continuously optimize the emergency response mechanism.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-65IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: IT Outsourcing / Vendor Management	3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	The outsourcing agreement should explicitly provide a clause allowing Bangko Sentral and BSFIs' internal and external auditors to review the operations and controls of the service provider as they relate to the outsourced activity.	The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual situation. Huawei Cloud will comply with the requirements specified in the agreements signed with BSFIs and assign dedicated personnel to actively cooperate with BSFIs and financial transaction entities to supervise and supervise the audit and supervision of Huawei Cloud.

6.8 APPENDIX— —Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Appendix Q-66 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Electronic Banking，Electronic Payment，Electronic Money and Other Electronic Products and Services	4. RISK MANAGEMENT CONTROLS	4.1.7. Infrastructure and Security Monitoring. The BSFI should establish an appropriate operating environment that supports and protects systems on e-services. It should proactively monitor systems and infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. The BSFI should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-services systems, servers,	Huawei Cloud provides infrastructure for customers and regards infrastructure security as the core component of building a multi-dimensional full-stack cloud security protection system. It provides multi-layer security protection in terms of physical environment, network, platform, application program interface, and data. Huawei Cloud builds a secure infrastructure foundation so that tenants can access the cloud with confidence and use secure Huawei Cloud services to focus on business development. Huawei Cloud uses the situational awareness analysis system to correlate alarm logs of various security devices and perform unified analysis to quickly and comprehensively identify attacks

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		databases, and applications.	that have occurred and predict threats that have not occurred. Supports multiple threat analysis models and algorithms, and uses threat intelligence and security consulting to accurately identify attacks. In addition, the system evaluates Huawei Cloud security status in real time, analyzes potential risks, and provides warnings based on threat intelligence to prevent attacks. In addition, the Huawei Cloud log big data analysis system can quickly collect, process, and analyze massive logs in real time. It can interconnect with third-party security information and event management (SIEM) systems, such as ArcSight and Splunk.
Appendix Q-66 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Electronic Banking，Electronic Payment，Electronic Money and Other Electronic Products and Services	4. RISK MANAGEMENT CONTROLS	4.1.8. Audit Trail. The BSFI should ensure that comprehensive logs are maintained to record all critical e-services transactions to help establish a clear audit trail and promote employee and user accountability. Audit logs should be protected against unauthorized manipulation and retained for a reasonable period （e.g. three months） to facilitate any fraud investigation and any dispute resolution if necessary.	Huawei Cloud's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. In addition, Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days.
Appendix Q-66 IT RISK MANAGE	4. RISK MANAGEMENT CONTRO	4.2.2. Incident Response and Management. The BSFI should put in place formal incident	Huawei Cloud has developed a security incident management mechanism, including a general security incident response plan and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
MENT STANDARDS AND GUIDELINES Area: Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services	LS	response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-services during or outside office hours. A communication strategy should be developed to adequately address the reported concerns and an incident response team	process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents. Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, Huawei Cloud can promptly notify financial institutions of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation.
Appendix Q-66 IT RISK MANAGEMENT STANDARDS AND GUIDELINES Area: Electronic Banking, Electronic Payment,	4. RISK MANAGEMENT CONTROLS	4.3.1. Customer Privacy and Confidentiality. The BSFI should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the institution is providing electronic products and services. Misuse or unauthorized disclosure of confidential customer	In each country and region, Huawei Cloud has dedicated legal affairs and privacy protection personnel to help Huawei Cloud activities meet applicable privacy laws and regulations. Customers have full control over their content data and act as responsible parties. Customers shall ensure that personal information is collected for specific, explicit, and legitimate purposes, inform data subjects of the purpose of collecting personal information, and obtain

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Electronic Money and Other Electronic Products and Services		data exposes the entity to both legal and reputation risk. To meet these challenges concerning the preservation of privacy of customer information， the BSFI should make reasonable endeavours to ensure that: ●The BSFI's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-services; ●Customers are made aware of the BSFI's privacy policies and relevant privacy issues concerning use of e-services; ●Customers may decline （"opt out"） from permitting the BSFI to share with a third party for cross-marketing purposes any information about the customer's personal needs， interests， financial position or banking activity; and ●Customer data are not used for purposes beyond which they are specifically allowed or for purposes beyond which customers have authorized. The BSFI's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.	data subjects' consent. Huawei Cloud does not touch customer content data, nor does it know for what purpose it was collected.

7 How Huawei Cloud Complies with and Assists Customers to Meet the Requirements of the "Circular No.982, Series of 2017, Guidelines on Information Security Management"

Circular No. 982, Series of 2017, Enhanced Guidelines on Information Security Management, which came into effect on November 9, 2017, amended the MORB and MORNBFI regulations on information security management to better adapt to rapidly evolving technology levels and respond to increasingly serious cyber threats. As a service provider, Huawei Cloud is affected by this revision in terms of risk management, cyber resiliency, and threat monitoring.

When BSFIs are seeking to comply with the requirements provided in the Enhanced Guidelines on Information Security Management (Circular No. 982), Huawei Cloud, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the Enhanced Guidelines on Information Security Management (Circular No. 982), and explains how Huawei Cloud, as a cloud service provider, can help BSFIs to meet these requirements.

7.1 Risk Management System

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3.IT Control Implementation	a. Information Security	3.IT Control Implementation a. Information Security. BSFI needs to put in place a robust, resilient and enterprise-wide framework for ISRM supported by effective information security governance and oversight mechanisms. An ISRM framework should	Huawei Cloud has built an information security management system based on the requirements of ISO27001, ISO27017, ISO27018, SOC, and CSA STAR, and has formulated the overall information security policies, management methods of information security system

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		be in place encompassing key elements and phases with effective governance mechanisms to oversee the entire process.	documents, and key information security directions and objectives. Huawei Cloud has established information security risk management regulations and developed an information security risk assessment method to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security. Based on the confidentiality, integrity, and availability of assets and business processes, it identifies Huawei Cloud threats and vulnerabilities and conducts risk ratings. The assessment is formally recorded and a risk disposal plan is formulated. 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.
3.IT Control Implementation	a. Information Security	3.(4) Cyber threat intelligence and collaboration. In response to the growing cyber-threat landscape, BSFIs need to step up their information security posture and resilience beyond their respective networks. Likewise, BSFIs need to enhance situational awareness that would provide a keen sense of	Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		the threat landscape. Further, BSFIs need to collaborate with each other, including regulators, law enforcement agencies, and other third party stakeholders for a collective, coordinated, and strategic response through information sharing and collaboration.	models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. 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. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability information, including the cloud, is immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed. In addition, Huawei Cloud is equipped with dedicated personnel to maintain contact and establish contact points with industry bodies, risk and compliance organizations, local authorities and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			regulators.

7.2 Information Security Field

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3. Information Security Planning Management	3.1	3.1.1. Risk Management Process. Management should conduct periodic security risk assessment to identify and understand risk on confidentiality, integrity and availability of information and IT systems based on current and detailed knowledge on BSFI's operating and business environment. This includes identifying information security risks relative to its internal networks, hardware, software, applications, systems interfaces, operations and human elements. The risk assessment should include an identification of information and IT resources to be protected and their potential threats and vulnerabilities. After which, the appropriate risk treatment options (i.e., mitigate, transfer, avoid or accept) should be applied taking into consideration the BSFI's risk appetite and tolerance. Once the BSFI identifies the risks	Huawei Cloud has established information security risk management regulations, clarify the key processes that should be followed in risk management, the scope of risk management, relevant departments responsible for risk management and the standards that should be followed in risk management, to identify risks from multiple dimensions, determine the possibility of risks based on the completeness of security policies, security technologies, security audits, and periodically assess information security risks are required. Risk assessment covers various aspects of information security. Based on the confidentiality, integrity, and availability of assets and business processes, it identifies Huawei Cloud threats and vulnerabilities and conducts risk ratings. The assessment is formally recorded and a risk disposal plan is formulated.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		to mitigate, Management can begin to develop risk mitigation strategy. The risk management phases from identification to risk treatment should flow into the BSFI's risk reporting and monitoring activities to ensure effectiveness and continuous improvement of the entire risk management process.	
3. Information Security Planning Management	3.2	3.2.3. Threats and Vulnerabilities. In identifying risks, the BSFI should have a documented process that will determine the threats and vulnerabilities to the institution's IT environment. As threats continue to evolve rapidly and increase in sophistication, Management should ensure that threat monitoring and vulnerability scanning tools and processes remain effective in identifying both known and unknown (zero-day) security exposures.	Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. 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, take necessary security precautions. Huawei Cloud has established a security vulnerability management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			process, which standardizes the closed-loop process of early warning, assessment, and repair processing of Huawei Cloud system security vulnerabilities, ensures the regular installation of critical security patches to reduce risks related to vulnerabilities, and define vulnerability rating, responsibility assignment and vulnerability handling requirements. Additionally, Huawei Cloud has built a privacy protection system based on global privacy protection laws and regulations and best practices widely recognized in the industry to protect privacy and personally identifiable information. On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. For all known security vulnerabilities, Huawei Cloud evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated. At the same time, Huawei PSIRT will actively monitor the industry's well-known vulnerability databases, security forums, mailing lists, security conferences and other channels to ensure that Huawei-related vulnerability information, including the cloud, is

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			immediately perceived. By building a company-level vulnerability library for all products and solutions, including cloud businesses, to ensure that every vulnerability is effectively documented, tracked, and closed.In addition, Huawei Cloud is equipped with dedicated personnel to maintain contact and establish contact points.
3. Information Security Planning Management	3.3	3.3.1.1. Policies, Standards, and Procedures. Management should formulate written information security policies, standards, and procedures which define the institution's control environment and guide employees on the required, expected, and prohibited activities. The Board and Senior Management should approve and periodically review policies, standards, and procedures to ensure ongoing alignment with business needs and requirements.	Huawei Cloud has established and implemented documented cyber security policies and procedures, It covers multiple security domains, including information security organization, human resource security, access control, physical and environmental security, operation security, communication security, system acquisition, development and maintenance, and information security events, to provide guidance for cyber security management. The release of cyber security policies and procedures must be approved by managers. Employees can view the released information security policies and procedures as authorized. In addition, Huawei Cloud regularly conducts employee training on corporate policies and culture every year.
3. Information Security Planning Management	3.3	3.3.1.1.1. Minimum Baseline Security Standards. Management should put in place minimum baseline security standards (MBSS) to ensure that	Huawei Cloud implements a series of network security controls on the physical environment, network, platform, application programming interfaces (APIs), and data to ensure

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		systems, hardware, and network devices are consistently and securely configured across the organization. These standards enable the deployment of operating systems, databases, network devices, and mobile devices within the IT environment in an efficient and standardized manner. Management may refer to leading standards and best practices as well as vendor-specific recommendations in developing their MBSS, taking into consideration the following controls: a. Secure configuration of operating systems, system software, databases, and servers to meet the intended uses with all unnecessary services and programs disabled or removed; b. Periodic checking to ensure that baseline standards are consistently complied with; c. Timely deployment of tested and approved patches and security updates; d. Adequate documentation of all configurations and settings of operating systems, system software, databases, and servers; and e. Adequate logging capabilities for all systems, applications,	secure infrastructure design and practice. a. Huawei Cloud has established unified baseline configuration standards for server operating systems, system software, database management systems, and network devices that supports service operation by referring to industry best practices to implement unified management of service baseline configurations and specify security configuration requirements for systems/components in the Huawei Cloud production environment, and ensure effective execution and continuous improvement of security configurations. b. The Huawei Cloud O&M team periodically checks and updates system security parameters based on internal security baseline management regulations. Huawei Cloud hardens the security configurations of host operating systems, VMs, databases, and web application components and periodically checks them. c. Huawei Cloud establishes a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. In addition, Huawei Cloud has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services, continuously optimize the default security configurations of cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		network devices, and databases.	platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period. d. Security baseline requirements are specified for all configurations and settings of Huawei Cloud OSs, system software, databases, and servers. All products are configured based on the baseline requirements specified in the cyber security redline formulated by Huawei Cloud to ensure that unnecessary functions are restricted. e. Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance.
3. Information Security Planning Management	3.3	3.3.1.2. Security Training and Awareness Programs. All employees of the organization and, where relevant, contractors and third party users should receive appropriate information security awareness training and regular updates in organizational policies and procedures relevant	Huawei Cloud has established its own training mechanism and designed appropriate training plans for employees based on different roles and positions. Huawei Cloud continues security awareness training for employees during their employment. There is a special information security awareness training program for employees. The training frequency for general

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		to their job function. Security training and awareness programs should be designed and tailored to the specific requirements of different groups and stakeholders (i.e., business process/information owners, security specialists, incident responders, etc.).	employees is at least once a year, and the training frequency for core employees is higher. This training includes but is not limited to, on-the-spot speeches and online video courses, information security presentation, and case study.
3. Information Security Planning Management	3.3	3.3.1.3. Security Screening in Hiring Practices. Management should have a screening procedures, including verification and background checks, should be developed for recruitment of permanent and temporary IT staff, and contractors, particularly for sensitive IT-related jobs or access level. Similar checks should be conducted for all staff, including contractors, at regular intervals throughout their employment, commensurate with the nature and sensitivity of their job functions as well as their access to critical systems. Further, it should establish processes and controls to mitigate risks related to employees' termination/resignation or changing responsibilities.	If permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Simultaneously, to ensure orderly internal management and reduce the potential impact of personnel management risks on business continuity and security, Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including onboarding security review, on-the-job security training and enablement, onboarding qualifications management, and off-boarding security review.
3. Information Security Planning Management	3.3	3.3.2. Physical and Environmental Controls. Physical security measures should be in place to protect	Huawei Cloud has established comprehensive physical security and environmental security protection measures,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		computer facilities and equipment from damage or unauthorized access that can impair the confidentiality, integrity, and availability of information. Critical information processing facilities should be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and upon presentation of proper identification and authentication process (i.e., ID cards, badges, biometrics, etc.). Moreover, a specific and formal authorization process should be employed for the removal of hardware and software from the premises. Since the data center houses the BSFI's most critical information processing facilities, Management should fully consider the environmental threats (e.g., proximity to dangerous environment hazards) when selecting sites for data centers. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities. Moreover, physical and environmental controls should be implemented	strategies, and procedures. Huawei Cloud data centers are located on suitable physical sites, as determined from solid site surveys. 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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		to prevent, detect, and monitor environmental conditions which could adversely affect the operation of information processing facilities (e.g., fire, explosives, smoke, temperature, water, and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and backup generators. Management should ensure that these systems and devices regularly undergo preventive maintenance to ensure that they are in good working condition and operating as intended.	
3. Information Security Planning Management	3.3	3.3.3.1. Technology Design. Management should consider information security and cyber resilience during the infrastructure build-up, systems development and product design. It should ensure that applicable standards and operating procedures are in place for all software, network configurations, and hardware connected to critical systems.	Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. Huawei Cloud and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			is identified, the design engineer will formulate mitigation measures according to the reduction library and the security design library and complete the corresponding security design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the security of products and services.
3. Information Security Planning Management	3.3	3.3.3.2. Identity and Access Management. The BSFI should adopt a sound and systematic identity and access management program following the principles of least privilege and segregation of duties. The BSFI should have an effective process to manage user authentication and access control consistent with the criticality and sensitivity of the information/system. The grant, modification, and removal of user access rights should be approved by the information/system owner prior to implementation. Information/system owners or business line managers should ensure that user access rights remain appropriate through a periodic user access re-certification	1) Huawei Cloud provides Identity and Access Management (IAM) for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication. IAM provides federation authentication for customers. Customers who have a reliable identity authentication service provider in place can map their federated users to IAM users in a specified period for access to customer's Huawei Cloud resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL),

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		process. Obsolete user accounts or inappropriate access rights should be disabled/removed from the systems in a timely manner. The BSFI should have password standards in place to ensure that user passwords are not easily compromised (i.e., password syntax, validity, system-enforced password changes). Stronger authentication methods, such as the use of multi-factor authentication techniques, should be deployed for high-risk transactions (e.g., large value funds/wire transfers, enrollment of billers, systems administration functions). Default user accounts defined in new software and hardware should either be disabled or changed and subject to close monitoring. Privileged access and use of emergency IDs should be tightly controlled as it gives the user the ability to override system or application controls.	to prevent malicious access from untrusted networks. Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. 2) Huawei Cloud has established Internal operation and maintenance account lifecycle management.It includes account management, account owner/user management, password management, account management monitoring, etc. Once created, new accounts are immediately scoped in for daily O&M by security administratorsAll operation and maintenance accounts, accounts of all devices and applications are managed in a unified manner, and are centrally monitored through a unified audit platform, and automatic auditing is performed to ensure the full process management from user creation, authorization, authentication to permission recovery. If the account user wants to use the account, the account administrator can start the authorization process, and authorize by password or by increasing the authority of the account; the applicant and the approver of the account cannot be the same person. Huawei Cloud implements role-based access control and permission management for internal personnel, restricting personnel with different positions and responsibilities to only perform specific operations on authorized

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			targets. Ensure that personnel do not gain unauthorized access through minimal privilege assignment and strict behavioral auditing. 3) 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. 4) O&M: At the same time, when Huawei Cloud O&M personnel access Huawei Cloud Management Network for centralized management of the system, they need to use only identifiable employee identity accounts. In addition, two-factor authentication is used to authenticate cloud personnel, such as USB key, Smart Card and so on. Employee account is used to log on VPN and access gateway to realize the deep audit of user login. Privileged Account Management System binds functional or technical accounts of daily or emergency operations to operation and maintenance teams or individuals. Strong log auditing is supported on the bastion host to ensure that the operation and maintenance personnel's operations on the target host can be located to individuals. Grant privileged or emergency accounts to employees only when necessary for their duties. All

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			applications for privileged or emergency accounts are subject to multiple levels of review and approval.
3. Information Security Planning Management	3.3	3.3.3.2.1. Remote Access. The BSFI, in line with business strategies and needs, may allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as "bring your own device" or BYOD). Management should ensure that such remote access is provided in a safe, secure, and sound manner to manage attendant risks. At a minimum, the BSFI should establish control procedures covering: a. Formal authorization process for granting remote access; b. Risk-based authentication controls for remote access to networks, host data and/or systems, depending on the criticality and sensitivity of information/systems; c. Securing communication channels, access devices and equipment from theft, malware and other threats (i.e., encryption, strong authentication methods, data wipe capabilities, application whitelisting1); and d. Logging and monitoring all remote access communications.	Huawei Cloud employees use unique identity in the internal office network. If the external network needs to be connected to HUAWEI working network, it is necessary to access through VPN. For O&M scenarios, centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. The data center external network operation and maintenance personnel and intranet operation and maintenance personnel centrally manage all local and remote operations of network, server and other equipment, and realize unified access, unified authentication, unified authorization, and unified auditing of equipment resource operation management by users. For remote management of Huawei Cloud, whether from the Internet or office network, it is necessary to first access the resource pool bastion host, and then access related resources from a bastion server.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3. Information Security Planning Management	3.3	3.3.3.3. Network Security. Management should adopt robust and multi-layered controls to prevent and detect unauthorized access, misuse, and other threats from entering and/or spreading into its internal computer networks and systems. Effective controls should be employed to adequately secure system and data within the network which include the following, among others: a. Grouping of network servers, applications, data, and users into security domains or zones (e.g., untrusted external networks, external service providers, or trusted internal networks); b. Adopting security policies for each domain in accordance with the risks, sensitivity of data, user roles, and appropriate access to application systems; c. Establishment of appropriate access requirements within and between each security domain; d. Implementation of appropriate technological controls to meet access requirements consistently; e. Monitoring of cross-domain access for security policy violations and	To simplify network security design, prevent the spread of network attacks on Huawei Cloud, and minimize the impact of attacks, Huawei Cloud divides and isolates security zones and services based on ITUE.408 security zone division principles and best cyber security practices in the industry. Nodes in a security zone have the same security level. Huawei Cloud network architecture design, device selection and configuration, and O&M are considered. Huawei Cloud uses multiple layers of security isolation, access control, and border protection technologies for physical and virtual networks, and strictly implements management and control measures to ensure Huawei Cloud security. Huawei Cloud divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. Huawei Cloud maintains the latest network topology. Huawei Cloud data centers are divided into five key security zones: DMZ, public service, POD-Point of Delivery, OBS-Object-Based Storage, and OM-Operations Management. In addition to the preceding network partitions, Huawei Cloud also divides the security levels of different zones and determines different attack

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		anomalous activity; and f. Maintaining accurate network diagrams and data flow charts. Commonly used tools and technologies to secure the network include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and demilitarized zones, among others. As the network complexity as well as threats affecting the network evolve, the BSFI should continuously monitor and enhance its network security and systems to ensure that they remain secure, safe, and resilient.	surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. Huawei Cloud isolates data on the cloud by using the Virtual Private Cloud (VPC). VPC uses the network isolation technology to isolate tenants at Layer 3 networks. Tenants can completely control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using VPNs or Direct Connects, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configure security and access rules on demand to meet tenants' fine-grained network isolation requirements. In terms of network border protection, Huawei Cloud has established a solid and complete border and multi-layer security protection system, and deployed Anti-DDoS, IDS/IPS, and WAF protection mechanisms. Anti-DDoS quickly detects and defends against DDoS attacks and comprehensively

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			defends against traffic attacks and application-layer attacks in real time. WAF detects and defends against web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately. The IDS/IPS detects and blocks network attacks from the Internet in real time and monitors abnormal host behaviors.
3. Information Security Planning Management	3.3	3.3.3.3.1. Virtualization. As BSFIs are increasingly leveraging on virtualization technologies to optimize existing hardware resources, reduce operating expenses and improve IT flexibility and agility to support business needs, additional security risks such as attacks on hypervisor integrity and lack of visibility over intra-host communications and virtual machine (VM) migrations are also rising. To address such risks, Management should extend security policies and standards to apply to virtualized servers and environment. Likewise, it should adopt the following control measures: a. Hypervisor hardening with strict access controls and patch management; b. Inspection of intra-host communications {traffic within VM environments) and	Huawei Cloud adopts a series of security mechanisms for VMs to cope with network security risks. The VM security of Huawei Cloud isolates the network from the platform. On the network layer, a virtual switch provided by the hypervisor on each host is used to configure VLAN, VXLAN, and ACL settings to ensure that the VMs on that host are logically isolated. UVP supports the configuration of security groups to isolate VMs by group. Tenants can create security groups containing multiple VMs to enable those VMs to access each other while maintaining isolation from other VMs. By default, VMs in the same security group can access each other but any two VMs in different security groups cannot access each other. That said, access and communication between any two VMs in different security groups can also be customized by the tenant. Huawei Cloud's professional security team performs security hardening on public images and patches any system vulnerabilities that

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		ensuring that security control measures are implemented for confidential/sensitive data stored in VMs; and c. VM creation, provisioning, migration, and changes should undergo proper change management procedures and approval processes similar to deployment of physical network/system devices and servers. The BSFI may also consider implementing next generation firewalls that can restrict access more granularly and prevent virtualization-targeted attacks that exploit known VM vulnerabilities and exploits.	may occur. Secure, updated public images are created with the help of an image factory and provided to users through Image Management Service (IMS). Pertinent hardening and patch information is also provided to tenants for reference during image testing, troubleshooting, and other O&M activities. When creating VMs, tenants can decide based on their applications and security policies whether to use an up-to-date public image or create a private image that has the required security patches installed.
3. Information Security Planning Management	3.3	3.3.3.5. Data Security. The BSFI should have information classification strategy guidelines and institute appropriate set of controls and procedures for information protection in accordance with the classification scheme. Information should be protected throughout its life cycle from handling, storage or data-at- rest, transmission or data-in-transit, up to the disposal phase. 3.3.3.5.1. Data-at-Rest. Policies, standards, and procedures as well as risk management controls must be in place to secure the BSFI's information	Huawei Cloud uses a series of protection mechanisms to protect tenant data storage security. First, Huawei Cloud provides Key Management Service (KMS). It helps users to centrally manage keys and protect key security. It uses a hardware security module (HSM-Hardware Security Module) to create and manage keys for tenants, preventing the key plaintext from being exposed outside the HSM, thereby preventing key leakage. The services that connect with Huawei Cloud KMS include OBS, cloud hard disk, etc. Secondly, in the encryption scenario where the exclusive encryption meets the higher compliance requirements of

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		assets, whether stored on computer systems, physical media, or in hard- copy documents. The level of protective controls shall depend on the sensitivity and criticality of the information. BSFI should exercise effective oversight over the cloud service provider in terms of adherence to security, performance and uptime, and back-up and recovery arrangements contained in the contract/agreement. 3.3.3.5.1.1. Database security. The BSFI should adopt policies, standards, and procedures to adequately secure databases from unauthorized access, misuse, alteration, leakage and/or tampering. Considering their criticality, sensitivity and business impact, access authorizations to databases should be tightly controlled and monitored. Databases should be configured properly and securely with effective preventive and detective controls such as encryption, integrity checkers, logs and audit trails, among others. 3.3.3.5.2. Data-in-transit. Data transfers are commonly done through physical media or electronic transmission. Policies,	the tenant, a hardware encryption machine certified by the State Cryptography Administration or FIPS140-2 Level 3 verification is used to perform exclusive encryption for the tenant's business, and the default dual-machine architecture is used to improve reliability. Finally, Huawei Cloud's various storage products such as EVS and VBS provide storage encryption mechanisms. Second, the storage and database services provided by Huawei Cloud are guaranteed to be highly reliable. For example, EVS cloud hard disk uses a multi-copy data redundancy protection mechanism, and adopts measures such as synchronous write and read recovery of copies to ensure data consistency. When hardware failure is detected, it can be automatically repaired in the background, data is quickly and automatically rebuilt, and data durability can reach 99.9999999% . ;OBS object storage service supports the high reliability of object data, and through the high reliability network of business nodes and the multi-redundancy design of nodes, the system design availability reaches 99.995%, which fully meets the high availability requirements of object storage services. Provides multiple redundancy of object data and automatic restoration technology to ensure the data consistency of multiple objects to provide high reliability of

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		standards, and procedures should be in place for maintaining the security of physical media containing sensitive information while in transit, including to off-site storage, or when shared with third parties. 3.3.3.5.2. Removal, Transfers and Disposition of Assets. Procedures for the destruction and disposal of media containing sensitive information should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Disposal techniques that the BSFI may implement include deletion, overwriting, degaussing1, destruction of the media. Management should be mindful about residual data being stored in computer-based media as well as dumpster-diving attacks in paper-based information in deciding the best disposal strategy for sensitive information assets.	object data. The system design data durability is as high as 99.9999999999%; RDS relational database service adopts hot standby architecture, failure system 1 minute automatic switching. Data is automatically backed up every day, uploaded to the OBS bucket, and the backup files are retained for 732 days. One-click recovery is supported. For database security, Huawei Cloud ensures database security through database security reinforcement and database security design. The database provided by Huawei Cloud has various features to ensure the reliability and security of the tenant database, such as VPC, security group, permission setting, SSL connection, automatic backup, database snapshot, point in time recovery (PITR-Point In Time Recovery), Deploy across Availability Zones and more to protect databases from unauthorized access, misuse, alteration, leaks and/or tampering. At the same time, customers can also use the database security service (DBSS) provided by Huawei Cloud. This service includes two functional modules: database security audit and database security protection. It provides three functions of database audit, data leakage protection, and database firewall, which can comprehensively protect the cloud. Database security. For the data in transit, the data from the client to the server and between the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			server on the Huawei Cloud platform is transmitted through a public information channel. The protection of the data in transit is through virtual private network (VPN) and application layer TLS and certificate management. , Huawei Cloud services provide customers with two access methods: console and API. Both use encrypted transmission protocols to build secure transmission channels, effectively reducing the risk of malicious sniffing of data during network transmission. For data security deletion, after the customer confirms the deletion of data, Huawei Cloud will comprehensively clear the specified data and all its copies. First, delete the index relationship between the customer and the data, and then delete the storage space such as memory and block storage. Perform a clearing operation before reallocation to ensure that the related data and information cannot be restored. When the physical storage medium is scrapped, Huawei Cloud clears the data by degaussing, bending, or breaking the storage medium to ensure that the data on it cannot be recovered.
3. Information Security Planning Management	3.3	3.3.3.6. Malware Protection. Management should adopt layered and integrated anti-malware strategy, including data integrity checks, anomaly detection, system behavior monitoring, and	Huawei Cloud implements comprehensive malware and virus protection mechanisms for the cloud platforms it is responsible for. In addition, Huawei Cloud uses the IPS, WAF, antivirus software, and HIDS host intrusion detection system to manage vulnerabilities of

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		enhanced employee security awareness training programs. At a minimum, Management should apply the "Least Privilege" principle in granting access to all systems and services and mandate safe computing practices for all users. Other preventive measures include installation and timely update of anti-malware software provided by reputable vendors, periodic vulnerability scanning, and effective patch management procedures for all critical systems and applications. To address the more sophisticated forms of malware, Management should consider adopting advanced security solutions such as signature-less anti malware solutions capable of analyzing abnormal behavioral patterns in network and system traffic flows. As malware sophistication and capabilities evolve, Management should continuously monitor changes in technologies, threat profiles and the overall operating environment to address emerging risks. It should likewise closely coordinate with its technology vendors and relevant information sharing groups for appropriate remediation	system components and networks. IPS can detect and prevent potential network intrusions. WAF is deployed at the network border to protect application software from external attacks such as SQL injection, CSS, and CSRF. Antivirus software provides antivirus protection and firewalls in Windows systems. The HIDS host-based intrusion detection system protects ECSs and reduces the risk of account theft. It provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page tamper protection. Huawei Cloud has established a periodic vulnerability scanning mechanism. Each month, the vulnerability scanning team scans products within the scope of the report, and the vulnerability scanning team tracks and processes the scanning results. In addition, On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. Huawei Cloud uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		procedures.	addition, Huawei Cloud has established a security vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability handling requirements. In addition, Huawei Cloud has established a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures. Huawei Cloud uses the situational awareness analysis system to correlate the alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not yet occurred. Supports numerous threat analysis models and algorithms, combined with threat intelligence and security consulting, to accurately identify attacks, including the most common cloud attack threats: brute force attacks, port scanning, zombie attacks (machines remotely controlled by hackers), web attacks, and unauthorized web access, and APT attack, etc. In addition, the system performs real-time evaluation of the security posture of Huawei Cloud,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping Huawei Cloud take necessary security precautions. Huawei PSIRT proactively monitors the industry's well-known vulnerability database, security forums, mailing lists, and security conferences to ensure that Huawei-related vulnerability information, including the cloud, is immediately detected. Establish a corporate-level vulnerability database for all products and solutions, including cloud services, to ensure that each vulnerability is effectively recorded, tracked, and closed.
3. Information Security Planning Management	3.3	3.3.3.7. Encryption. Encryption, when properly designed, managed, and implemented, can serve as a key control in securing communications, information, and data storage. Management should adopt a sound encryption program covering the following elements: a. Encryption type, level and strength commensurate to the sensitivity of the information based on the institution's data classification policy; b. Effective key management policies and practices to properly safeguard the generation, distribution,	Huawei Cloud establishes an encryption policy and key management mechanism for protecting data on technical devices, and specifies the rights and responsibilities of personnel, encryption levels, and encryption methods. For encryption, Huawei Cloud uses the AES encryption method widely used in the industry to encrypt data on the platform. In the scenario where data is transmitted between clients and servers and between servers of the Huawei Cloud via common information channels, data in transit is protected by VPN and TLS and certificate management. Huawei Cloud provides customers with two access modes: console and API. Both use encrypted transmission protocols to construct secure transmission

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		storage, entry, use, and archiving of cryptographic keys; and c. Periodic review and testing to ensure that encryption methods deployed still provide the desired level of security vis-à-vis changes in technology and threat landscape.	channels. For key management, Huawei Cloud service domains must comply with key management security regulations and implement security control over key generation, key storage, key distribution, key update, and key destruction to prevent key leakage and damage. Huawei Cloud provides the Key Management Service (KMS). Key Management Service (KMS) is a secure, reliable, and easy-to-use key escrow service that facilitates centralized key management in order for users to achieve better key security. The KMS employs Hardware Security Module (HSM) technology for key generation and management, preventing the disclosure of plaintext keys outside HSM.
3. Information Security Planning Management	3.3	3.3.3.8. Integration with IT Processes. 3.3.3.8.1. Systems Development and Acquisition. Security requirements and considerations should be deeply embedded into the BSFI's systems development and acquisition processes. Aside from business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking, and exception handling should be clear and	Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. Huawei Cloud and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		specific. The information and/or process owners should check security requirements and conduct user acceptance tests prior to approval of systems to be loaded into the production environment. Further, BSFIs should maintain separate environments for their development, testing, and production activities respectively. In line with this, programmers/developers should have no access to the production environment. Lastly, strict segregation of duties between developers/programmers and IT operations should be upheld.	the design engineer will formulate mitigation measures according to the reduction library and the security design library and complete the corresponding security design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the security of products and services. 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 prevent security risks in the production environment caused by intrusion of the test environment. In addition, Huawei Cloud complies with the principles of separation of duties (SOD) and rights checks and balances, and separates incompatible responsibilities to ensure the separation of responsibilities between development and O&M personnel.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3. Information Security Planning Management	3.3	3.3.3.8.2. Change Management. The BSFI should have an effective and documented process to introduce changes into the IT environment in a safe and secure manner. Such changes should be controlled as to requirements definition, authorization and approvals, testing procedures, and audit trails. Moreover, the process should incorporate review of the impact of changes to the effectiveness of security controls.	Huawei Cloud has formulated management regulations and change procedures. All changes need to be fully validated before application with tests such as production environment tests, gray release tests, and blue-green deployment. This make that the change committee has a clear understanding of the change, the timeframe, the possible rollback of the change, and all possible impacts. In addition, Huawei Cloud has developed finer-grained change operation specifications to guide the implementation, tracking, and verification of the change, ensuring that the change achieves the expected purpose.Changes can be released only after achieving the approval of Huawei Cloud Change Committee.
3. Information Security Planning Management	3.3	3.3.3.8.3. Patch Management. Management should adopt a patch management process to promptly identify available security patches to technology and software assets, evaluate criticality and risk of patches, and test and deploy patches within an appropriate timeframe.	Huawei Cloud uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In addition, Huawei Cloud has established a security vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			handling requirements. In addition, Huawei Cloud has established a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures.
3. Information Security Planning Management	3.3	3.3.3.8.4. Vendor Management and Outsourcing. Management should conduct appropriate due diligence and consider information security in selecting third party service providers（TPSPs）. The BSFI should ensure that effective oversight processes are in place to monitor the activities of TPSPs. Contracts should sufficiently detail information security requirements, particularly for TPSPs that store, transmit, process, or dispose of customer information. Mechanisms should be in place to properly monitor the performance of third party service providers to confirm whether sufficient level of controls is maintained.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation. Huawei Cloud will comply with the security requirements specified in the agreement signed with the customer. Huawei Cloud will assign dedicated personnel to actively cooperate with the customer in the due diligence, supervision, and risk assessment on Huawei Cloud. Within Huawei Cloud, Huawei Cloud has established a supplier selection and monitoring system, and standardizes that R&D personnel manage suppliers' compliance with Huawei Cloud requirements and contract obligations through due diligence before

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			contract signing and periodic evaluation after contract signing.
3. Information Security Planning Management	3.4	3.4. Detection. Management should design and implement effective detection controls over the BSFI's networks, critical systems and applications, access points, and confidential information. Detection controls provide the institution with alerts and notifications for any anomalous activities within its network that can potentially impair the confidentiality, integrity, and availability of information assets. Detection controls which Management may employ include intrusion detection systems (IDS), virus/malware detection, honeypots, system alerts/notifications, and security incident and event management (SIEM) system.	Huawei Cloud employs its situation awareness 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. Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components, continuous monitoring and real-time analysis ensure the timely detection of security incidents.
3. Information Security Planning Management	3.4	3.4.1. Log Management. Log files can be analyzed for real-time or near real-time detection of anomalous activities, facilitate subsequent investigation of security incidents and can serve as forensic evidence for the prosecution of fraudulent activities. Thus, Management should put in place adequate security	Huawei Cloud uses a centralized log big data analysis system to collect management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. The logs are retained for more than 180 days. Security measures are taken during log storage to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		controls to prevent unauthorized access, modification and/or deletion of log files. Depending on the criticality of information contained in the log files, Management should implement the following controls to secure the integrity of log files: a. Encrypting log files containing sensitive data, where feasible; b. Ensuring adequate storage capacity to avoid gaps in log generation; c. Restricting access and disallowing modification to log files. Attempts to tamper with log files should prompt activation of system alarms/notifications; and d. Securing backup and disposal of log files.	prevent logs from being tampered with to ensure that cyber security event backtracking and compliance are supported. To ensure log data security, security logs are backed up or archived in a unified manner. According to data security management requirements, security log application and permission are restricted. Only authorized personnel can query security logs for necessary reasons to ensure controlled use. In addition, CTS records operations on cloud service resources for tenants. Many products and services also provide the log recording function. Tenants can select the log retention period based on their requirements to effectively support abnormal activity analysis.
3. Information Security Planning Management	3.4	3.4.2. Layered Detection. In designing the BSFI's detection controls and monitoring capabilities, Management should, to the extent feasible, adopt a layered or defense-in depth approach to ensure that a failure in one control would be compensated by another control.	The Huawei Cloud data center has many nodes and complex functional areas. To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			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. Among them, border protection also includes Anti-DDoS, network intrusion detection and Web security protection.
3. Information Security Planning Management	3.5	3.5. Response. Management should develop comprehensive, updated, and tested incident response plans supported by well-trained incident responders, investigators, and forensic data collectors. Through adequate response capabilities, Management should be able to minimize and contain the damage and impact arising from security incidents, immediately restore critical systems and services, and facilitate investigation to determine root causes. 3.5.1. Incident Response Plan and Procedures. Management should develop and implement a formal incident response plan to address identified information security incidents in a timely manner. 3.5.2. Incident Management Process. Incident handling should follow a	Huawei Cloud has developed a security incident management mechanism, including a general security incident response plan and process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents. Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, Huawei Cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		well-defined and documented incident management process which sufficiently details the steps from incident analysis and triage assessment, impact mitigation and containment up to testing and continuous improvements. 3.5.2.1. Incident Analysis and Triage Assessment. Reported incidents should be investigated to confirm their occurrence and classification. 3.5.2.2. Impact Mitigation and Containment. Upon discovery of an information security incident, the BSFI should seek to contain the damage, mitigate its effects, and eradicate the cause of the incident. Containment measures should be implemented to prevent further harm to the BSFI and/or its customers. 3.5.2.3. Testing and Continuous Improvement. Management should define a process for periodically reviewing the incident response plan and updating it based on the BSFI's experience from current and previous incident response activities, including periodic testing exercises.	can promptly notify financial institutions of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation. Huawei Cloud trains and tests information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training to ensure that critical incidents can be handled in a timely manner. In addition, security responders perform forensic analysis when a server/application is suspected to have been compromised. Huawei Cloud periodically collects statistics on incidents and analyzes the trend. For similar incidents, the problem handling team will find the root causes and develop solutions to prevent such incidents from occurring.
3. Information Security Planning	3.5	3.5.3. Incident Response Teams. The incident response plan should	Huawei Cloud has developed a security incident management mechanism,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Management		identify in advance the personnel who will be tasked to respond to an information security incident and clearly define their roles and responsibilities. In this regard, BSFIs should set-up and organize a formal security incident response team (SIRT) tasked to perform, coordinate, and support responses to security incidents and intrusions. Typical SIRT membership includes individuals with varied backgrounds and different areas of expertise including management, legal, public relations, information security, and information technology.	including a general security incident response plan and process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents.
3. Information Security Planning Management	3.5	3.5.4. Crisis Communication and Notification. The plan should be adequately communicated to appropriate internal and external stakeholders. The BSFI should establish and communicate standard procedures for reporting possible information security incidents to a designated officer or organizational unit.	Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			incident is resolved, the incident report will be provided to the customer according to the specific situation. Huawei Cloud is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies，reporting incident to regulatory institutions according to the requirements.
3. Information Security Planning Management	3.5	3.5.5. Forensic Readiness. Management should implement appropriate controls to facilitate forensic investigation of incidents. Policies on system logging should be established covering the types of logs to be maintained and their retention periods. Management should define in the response plan a systematic process for recording and monitoring information security incidents to facilitate investigation and subsequent analysis. Adequate documentation should be maintained for each incident from identification to closure.	Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. Huawei Cloud 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.
3. Information Security	3.6	3.6. Recovery. The BSFI should be able to	Huawei Cloud follows ISO 22301 international

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Planning Management		establish back-up facilities and recovery strategies to ensure the continuity of critical operations. During recovery phase, Management should ensure that information processed using back-up facilities and alternate sites still meet acceptable levels of security.	standards for business continuity management and has established a complete set of business continuity management systems. Within this framework, business impact analysis and risk assessment are carried out regularly, and comprehensive recovery policies are formulated for key services that support continuous running of cloud services. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of he affected area when compliance policies are met, ensuring service continuity. To meet the level of security acceptable to the customer during the recovery phase.
3. Information Security Planning Management	3.6	3.6.1. Business Continuity Management. Management should develop and implement a formal incident recovery plan to restore capabilities or services	Huawei Cloud has formulated business continuity management regulations to standardize the business continuity management framework, purpose and scope, management objectives,

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		that are affected by information security incidents in a timely manner. This can be achieved by incorporating scenarios related to information security (e.g., data breach, malware outbreak, denial of service) in its business continuity and disaster recovery plans.	roles, and responsibilities. Huawei Cloud has passed the ISO22301 Business Continuity Management System certification and has developed a business continuity plan and disaster recovery plan. Business continuity plans focus on major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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.
3. Information Security Planning Management	3.6	3.6.2. Communication Plan. A communication plan for information security incidents should be incorporated in the incident recovery plan to facilitate escalation for appropriate management action and to help manage reputation risk. Incidents that lead to publicly visible disruption to BSFI	Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events such as a severe service interruption occurs on the underlying infrastructure platform and have or may have a serious impact on multiple

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		services should be given utmost attention. Timely notification should be given to all relevant internal and external stakeholders (e.g., employees, customers, vendors, regulators, counterparties, and key service providers, media and the public) following a disruption.	customers, Huawei Cloud can promptly notify customers of service interruption event with an announcement. The contents of the notification include but are not limited to a description of the interruption event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the interruption incident is resolved, the incident report will be provided to the customer according to the specific situation.
3. Information Security Planning Management	3.6	3.6.3. Cyber Resilience. Management should consider the potential impact of evolving cyber events into the BSFI's business continuity planning and institute adequate cyber resilience capabilities. Given the unique characteristics of cyber-threats and attacks, traditional back-up and recovery arrangements adopted may no longer be sufficient. In some instances, it may even exacerbate the damage to BSFI's network, operations, and critical information assets. Hence, Management must consider cyber-related attacks and incidents in the BCM and recovery processes to achieve cyber resilience. 3.6.2.1. Business Impact Analysis/Risk Assessment. Management should	1) Business Impact Analysis/Risk Assessment. To provide continuous and stable cloud services to customers, Huawei Cloud has established a set of complete business continuity management systems in accordance with ISO 22301 - Business Continuity Management International standards. Under the requirements of this framework, Huawei Cloud carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. Huawei Cloud regularly conducts risk assessment according to the requirements of the internal business continuity management system, identifies and analyses the potential risks faced by key

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		consider the impact of cyber-threat scenarios during the Business Impact Analysis/Risk Assessment （BIA/RA） phase in conjunction with the ongoing information security risk assessment process. The BSFI should take into consideration a wide-range of cyber-threat scenarios perpetrated from diverse threat sources （e.g., skilled hackers, insiders, state-sponsored groups） which seek to compromise the confidentiality, availability, and integrity of its information assets and networks. Cyber-risks and threats such as malware, distributed denial of service （DDoS） attacks, advance persistent threats （APTs）, among others, should be considered in the BIA/RA process. 3.6.2.2. Defensive Strategies. Depending on the results of its risk assessments and cybersecurity profile, the BSFI may need to deploy defensive strategies ranging from basic to highly advanced technologies to promote cyber resilience, such as, defense-in-depth or layered controls, reducing attack surfaces, virtual technologies, air-gap facilities and threat intelligence feeds, among others.	resources supporting the continuous operation of cloud services, which includes network risks of service interruption, malware, distributed denial of service (DDoS) attacks, advanced persistent threats (APT) and so on. 2) Defensive Strategies. Huawei Cloud provides customers with infrastructure, Huawei Cloud considers infrastructure security to be a core component of its multi-dimensional full-stack cloud security framework. Provides multi-layer security protection in physical environments, networks, platforms, application program interfaces, and data, and builds a multi-dimensional, defense-in-depth, and compliance-compliant infrastructure architecture. It supports and continuously improves common cloud services with excellent security functions, as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) cloud services. For more information, see chapter 5 "Infrastructure Security" in the Huawei Cloud Security White Paper. To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		3.6.2.3. Recovery Arrangements. Depending on IT and operations risk profile and complexity, Management should consider adopting innovative recovery arrangements that address the unique risks arising from cyber-threats. These include the use of non-similar facility, cloud-based disaster recovery solutions and pre-arranged third party forensic and incident management services.	security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Huawei Cloud deploys Anti-DDoS devices, IPS devices, and web application firewalls at the network boundary to protect the boundary. Anti-DDoS devices can detect DDoS attacks, and IPS has the ability to analyze and block real-time network traffic, and can prevent exceptions. Protocol attacks, brute force attacks, port/vulnerability scanning, virus/Trojan horses, exploits targeting vulnerabilities and other intrusion behaviors. External firewalls can deal with external types of attacks, such as SQL injection, cross-site scripting attacks, and component vulnerabilities. For details, see the Huawei Cloud Security White Paper. 3) Recovery Arrangements. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.
3. Information Security Planning Management	3.7	3.7.2. Types of Tests and Evaluations. Considering that no one type of assessment can provide a complete representation of the BSFI's information security posture, Management should employ a variety of effective testing methodologies and practices in order to validate the overall effectiveness of the ISP. Some of the more common types of security assessment/testing with corresponding objectives, brief description and other details, in order of increasing complexity, are as follows: b. Security Audit/Review and Compliance Check — is commonly performed by the BSFI's IT auditors, security personnel, and compliance function, respectively, to assess compliance to relevant security policies,	Huawei has developed the internal audit management process to standardize the internal audit principles, audit management process, and audit frequency. Huawei Cloud has a dedicated audit team to perform an internal audit every year. The audit team checks the running status of the company's internal control system and evaluates the compliance and effectiveness of policies, procedures, and supporting measures and indicators. In addition, Huawei Cloud receives audits from professional third-party audit organizations every year and provides dedicated personnel for assistance. Huawei Cloud will arrange dedicated personnel to actively respond to and cooperate with customers in monitoring and auditing Huawei Cloud.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		standards, and procedures. Internal or external auditors review all aspects of the ISP to determine its overall effectiveness in achieving the desired security results or outcome. Auditors must have the necessary background, training, experience, and independence to effectively discharge their tasks and responsibilities.	
3. Information Security Planning Management	3.7	c. Vulnerability Assessment (VA) — refers to the identification of security vulnerabilities in systems and network usually through the use of automated vulnerability scanners. Frequency of the performance of vulnerability scans should be determined based on assessment of risk and criticality of systems or information stored on each system. High risk vulnerabilities uncovered during VA exercises should be remediated within a reasonable timeframe.	To meet customers' compliance requirements, Huawei Cloud regularly conducts internal and third-party vulnerability scan, penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. For all known security vulnerabilities, Huawei Cloud evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated.
3. Information Security Planning Management	3.7	d. Penetration Testing (PT) — involves subjecting a system or network to simulated or real-world attacks that exploit vulnerabilities under controlled	Huawei Cloud organizes internally or external third parties with certain qualifications to conduct penetration tests on all Huawei Cloud systems and applications every six

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		conditions. Depending on the test objectives and scope, the BSFI may use penetration testing to assess potential business impact, the level of security, risk management processes and controls as well as the knowledge of concerned personnel in the organization in identifying, detecting, and responding to attacks.	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.
3. Information Security Planning Management	3.7	e. Scenario-Based Testing - constitutes a wide range of scenarios, including simulation of extreme but plausible events such as targeted cyber-attacks in testing the BSFI's response, resumption and recovery practices, including governance arrangements and communication plans. To ensure robustness of test scenarios, cyber threat intelligence and threat modeling should be utilized to the extent possible to mimic actual cyber-threats and events.	The test scenarios will be based on common cyber security threats, and high-risk scenarios will be tested. During the test, Huawei Cloud selects test scenarios, formulates complete test plans and procedures, and records test results. After the test is complete, the related personnel prepare the test report to summarize the problems found during the test. At the same time, if the test results show that there are deficiencies in the information security incident management procedures and processes, the relevant documents will be updated.
3. Information Security Planning Management	3.7	f. Compromise/Breach Assessment — involves the placement of sensors/tools within the network to actively probe network traffic and system activities to detect, alert, and potentially mitigate malware intrusions as they occur. This type of assessment addresses	Huawei Cloud regularly conducts risk assessments to identify potential threats and vulnerabilities in its information and IT resources, and assess risks that need to be accepted or mitigated. Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		advanced malwares and threats with capabilities to evade traditional monitoring systems.	third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. Huawei Cloud collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. Continuous monitoring and real-time analysis ensure timely detection of security events. Huawei Cloud deploys Anti-DDoS devices, IPS devices, and web application firewalls at the network boundary to protect the boundary. Anti-DDoS devices can detect DDoS attacks, and IPS has the ability to analyze and block real-time network traffic, and can prevent exceptions. Protocol attacks, brute force attacks, port/vulnerability scanning, virus/Trojan horses, exploits targeting vulnerabilities and other intrusion behaviors. External firewalls can deal with external types of attacks, such as SQL injection, cross-site scripting attacks, and component vulnerabilities and so on.
3. Information Security Planning Management	3.7	g. Red-Teaming Exercise — a more in-depth type of penetration testing which continually challenges the organization's defenses and controls against	Huawei Cloud 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		cyber¬attacks. The red team is composed of highly-trained specialists, acting on adversarial mode, which may be the BSFI's own independent employees or third party experts. The end objective is to improve the state of readiness of the entire organization in cases of cyber-attacks.	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.
4.Cyber threat intelligence and collaboration	4.1	4.1. Situational Awareness and Threat Monitoring. In response to rapidly-evolving, sophisticated, and coordinated cyber-attacks targeting financial institutions, BSFIs need to enhance situational awareness as well as their threat monitoring capabilities. BSFIs should establish a systematic process of gathering, analyzing, and monitoring threat information for actionable intelligence, timely insights, and proactive response.	Huawei Cloud employs its situation awareness 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. Huawei Cloud can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. Huawei Cloud collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. Continuous monitoring and real-time analysis ensure timely detection of security events. Huawei PSIRT has established a comprehensive vulnerability awareness and collection channel. The vulnerability collection email address psirt@huawei.com and the vulnerability reward

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			program https://bugbounty.huawei.com/hbp have been published on PSIRT's official website, encouraging global vulnerability coordination organizations, suppliers, security companies, organizations, security researchers, and Huawei employees to submit vulnerabilities in Huawei products or solutions. At the same time, 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. A corporate-level vulnerability database covering all Huawei products, services and solutions, Huawei Cloud included, has been created to ensure the effective logging, tracking, resolution and closure of each and every vulnerability.
4.Cyber threat intelligence and collaboration	4.1	4.1.1. Security Operations Center. Centralizing security operations through a security operations center (SOC}, equipped with automated security monitoring tools, defined processes and highly-trained personnel, enables BSFIs to keep pace with the tactics of advanced threat actors. Considering that it may be difficult for some organizations to establish a mature and	Huawei Cloud employs its situation awareness 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. Huawei Cloud can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. The system collects management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		fully-operational SOC with the requisite skills, expertise and tools, the BSFI may opt to outsource some or all of its SOC functions to a third party service provider. This may be under a managed security service arrangement either on-premise, off-premise or through cloud computing platforms. In this regard, Management should exercise adequate oversight, due diligence and other risk management controls, and comply with existing Bangko Sentral regulations on outsourcing and cloud computing.	behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components, continuous monitoring and real-time analysis ensure the timely detection of security incidents. Huawei Cloud has developed a security incident management mechanism, including a general security incident response plan and process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents. Huawei Cloud has established a security incident response team to monitor and analyze alarms and assess whether they are information security incidents.
4.Cyber threat intelligence and collaboration	4.3	4.3. Information Sharing and Collaboration. With the stealthier, sophisticated and advanced forms of cyber-threats and attacks confronting the financial services industry, BSFIs should have a collective, coordinated, and strategic response through information	Huawei Cloud has formulated the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		sharing and collaboration. Information sharing allows BSFIs to enhance threat intelligence/ situational awareness that enable quick identification, prevention, and response to emerging and persistent threats. In some cases, BSFIs may need to cooperate with concerned government/regulatory bodies, law enforcement agencies and third party providers to prosecute cyber-criminals, activate government incident response plans or issue warnings/advisories to the public. The extent, breadth, and nature of information sharing activities of BSFIs largely depend on their maturity and capabilities. Moderate to Complex BSFIs should actively engage in information sharing organizations and fora within the financial services industry. At a minimum, BSFIs should define information sharing goals and objectives aligned with their ISSP and ISP. Further, BSFIs should formulate policies and procedures on information sharing activities within and outside their organizations.	multiple customers, Huawei Cloud can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation. Moreover, Huawei Cloud is designated with dedicated personnel to maintain contact and establish contact points with industry institutions, risk and compliance organizations, local authorities, and regulatory agencies. Huawei 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. A corporate-level vulnerability database covering all Huawei products, services and solutions, Huawei Cloud included, has been created to ensure the effective logging, tracking, resolution and closure of each and every vulnerability.

8 How Huawei Cloud Complies with and Assists customers to Meet the Requirements of the "Circular No.951, Series of 2017, Guidelines on Business Continuity Management "

Circular No. 951, Series of 2017, Guidelines on Business Continuity Management, issued by the Central Bank of the Philippines became effective on March 20, 2017. The Guide mainly addresses the provisions on business continuity management in MORB and MORNBFI. As a service provider, Huawei Cloud is affected by this revision in terms of system dependency.

When BSFIs are seeking to comply with the requirements provided in the Guidelines on Business Continuity Management (Circular No. 951), Huawei Cloud, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the Guidelines on Business Continuity Management (Circular No. 951), and explains how Huawei Cloud, as a cloud service provider, can help BSFIs to meet these requirements.

8.1 Plan Development

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Section5.	a	a. Business Impact Analysis and Risk Assessment. A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		work-flow analyses, enterprise-wide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies。	Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies.
Section5.	b	b. Strategy Formulation. Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required seb. Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA should be defined, approved, and tested. (1) Recovery Strategy. As business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure systems availability and recoverability during disruptions as prescribed under Appendix 75d of the MORB and Q-59d of the MORNBFI. Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels.	The customer should consider developing a recovery strategy based on the results of the business impact analysis. To help customers meet compliance requirements, Huawei Cloud formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			customer applications and data out of the affected area when compliance policies are met, ensuring service continuity.
Section 5.	c	1. BSFI should establish business continuity plan. The plan should include, at a minimum, the following components: （1） Escalation, declaration and notification procedures; （2） Responsibilities and procedures to be followed by each continuity or recovery teams and their members; （3） A list of resources required to recover critical processes in the event of a major disruption; （4） Relevant information about the alternate and recovery sites; （5） Procedures for restoring normal business operations. 2. BSFI should include a communication plan for notifying all relevant internal and external stakeholders following a disruption. 3. A crisis management plan should be included in the BCP. When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve	Customer should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. To provide continuous and stable cloud services for Customer, Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Based on the requirements of this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. To help Customer meet compliance requirements, Huawei Cloud develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on this, Huawei Cloud develops a business continuity plan and conducts regular tests. Business continuity plan (BCP) applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		successful BCP deployment.	Cloud services and safeguards customers' service and data security. Huawei Cloud has a disaster recovery 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. In addition, Huawei Cloud has established a crisis communication plan to promptly disclose related incidents and notify customers in accordance, and implement emergency plans and recovery processes to minimize the impact on services in the event of an emergency that affects customer service continuity. Every year, Huawei Cloud conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If the customer requires Huawei Cloud to participate in the development and execution of its business continuity plan, Huawei Cloud will actively cooperate with the customer.

8.2 Interdependence

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Section 6.	d	a. Pandemic Planning. Similar to natural disasters or technical disruptions, pandemics may also interrupt a BSFI's business activities. However, the difficulty in determining a pandemic's scope and duration present additional challenges in ensuring resilience and continuity of a BSFI's operations. Generally, pandemic plans are integrated in the BSFI's BCP and follows the same BCM process with additional considerations, such as: (1) Business Impact Analysis and Risk Assessment. The BCM process should consider pandemics as early as the BIA and risk assessment phase. The BIA and risk assessment should be updated to incorporate complexities that may arise from pandemics, such as (a) increasing level of absenteeism based on a pandemic's severity; and (b) the need for another layer of contingency plans as regular disaster or emergency response methods are no longer feasible. (2) Strategy formulation. To complement strategies for natural and technical disruptions, the following should be given due consideration when planning for pandemics: (a) Trigger events — Trigger events and strategies should be defined depending on the nature of a pandemic. Pandemic planning should have the flexibility to accommodate varying degrees of epidemic or outbreak as pandemics normally occur in waves or phases	Huawei Cloud has developed a business continuity management system that meets its service characteristics and has obtained the ISO22301 certification. Under this system framework, Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objective and minimum recovery level of key services. When identifying key services, the impact of service interruption on customers is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also develops corresponding business continuity plans and disaster recovery plans, and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. A disaster recovery plan refers to, for example, taking the cloud platform infrastructure and cloud services in a geographical location or region offline, simulating a disaster, and then performing system processing and transfer according to the disaster recovery plan to verify the services and operation functions of the faulty location. The test results are annotated and recorded for archiving. for continuous improvement of the program.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and of varying severity. (b) Remote access capability — In the event of a pandemic, enabling remote access may be one of the primary strategies available to a BSFI. To support a telecommuting strategy, the BSFI should ensure adequate capacity, bandwidth and authentication mechanisms in its technological infrastructure against expected network traffic or volume of transactions. (c) External parties — With pandemics not limited to the BSFI, establishing working relationships with external parties is an essential component. In addition to the communication plan for all relevant internal and external stakeholders, the BSFI should establish open relationships and communication channels with local public health and emergency response teams or other government authorities. The BSFI should inform concerned parties of any potential outbreaks and, at the same time, be aware of any developments in the expected scope and duration of a pandemic. (d) Employee awareness — As information becomes available from reputable sources or local agencies, the BSFI should ensure that steps to limit or reduce the risk of being affected by the pandemic are cascaded to its employees. (3) Plan Development. Pandemic plans should be commensurate to the nature, size and complexity of a BSFI's business activities and have sufficient flexibility to address the various scenarios that may arise. At a minimum, the pandemic plan should include: (a) Strategy that is scalable dependent on the extent and depth	

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		of the outbreak; (b) Preventive measures, including monitoring of current environment and hygiene tools available to employees; (c) Communication plan with internal and external stakeholders, including concerned local public health teams and government agencies; and (d) Tools, systems and procedures available to ensure continuity of its critical operations even with the unavailability of BSFI's staff for prolonged periods. (4) Plan Testing. Test policy/plan should include strategies to assess capability to continue critical operations, systems and applications even in the event of a severe pandemic. When regular tests are unable to cover pandemic scenarios, separate pandemic plan tests should be carried out. (5) Personnel Training and Plan Maintenance. The plan should be updated as developments and information become available. As needed, employee training programs should cover pandemic risks, including the roles and responsibilities of each employee during pandemic situations.	
Section 6.	d	d. Interdependence. An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. The BSFI may have very complex operating and recovery environment wherein interdependencies need to be duly considered, such as telecommunications, third party service providers, and recovery site. Given the critical resources	Customer should consider developing a recovery strategy based on the results of the business impact analysis. To help customers meet compliance requirements, Huawei Cloud formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		and services that are being shared with the BSFI or other entities, additional mitigating controls and recovery strategies need to be integrated in the plan.	systems, and third parties. Huawei Cloud can replicate and store user data on multiple nodes in a data center. Once a single node is faulty, user data will not be lost and the system can automatically detect and recover. Data Center Interconnect (DCI) is implemented between different AZs in a single region through high-speed optical fibers, meeting basic requirements for cross-AZ data replication. Users can select DR replication services based on service requirements. In addition to providing high-availability infrastructure, redundant data backup, and availability zone DR, Huawei Cloud also develops a business continuity plan and periodically tests the plan.

8.3 Outsourcing

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
Section 6.	h	h. Outsourcing. When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations.	Huawei Cloud has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Huawei Cloud periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on Customer is considered as an important criterion for determining key services. In addition, Huawei Cloud regularly assesses business continuity risks, identifies key risks that may cause

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			cloud service interruption, and formulates corresponding risk mitigation strategies. Based on these risks, Huawei Cloud also establishes corresponding business continuity plans and conducts regular tests to ensure customer security. Business continuity plans are designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. Huawei Cloud has a Disaster Recovery 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.

9 How Huawei Cloud Complies with and Assists Customers to Meet the Requirements of "Circular No. 808, Series of 2013, Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions"

Circular No. 808, Series of 2013, Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions, issued by Bangko Sentral ng Pilipinas (BSP)，came into effect on 22 August 2013, mainly revised the MORB's provisions on information technology risk management. As a service provider, Huawei Cloud is affected by this revision in terms of audit, information security, project management, development, procurement, change management, IT operations, IT outsourcing/vendor management, e-banking, e-payment, e-money, and other electronic products and services..

When BSFIs are seeking to comply with the requirements provided in the Series of 2013, Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions (Circular No. 808), Huawei Cloud, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the Series of 2013, Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions (Circular No. 808), and explains how Huawei Cloud, as a cloud service provider, can help BSFIs to meet these requirements.

9.1 Technology Risk Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
176.7	1. IT Governance.	b. IT Policies, Procedures and Standards. IT policies and procedures should include at	Huawei Cloud has established a comprehensive IT risk system based on international and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		least the following areas: 1）IT Governance/Management; 2）Development and Acquisition; 3）IT Operations; 4）Communication networks; 5）Information security; 6）Electronic Banking/Electronic Products and Services; 7）IT Outsourcing/ Vendor Management.	industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. 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 files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity.
176.7	1. IT Governance.	c.IT audit. BSFI should establish effective audit programs and periodic reporting to the Board on the effectiveness of institution’s IT risk management, internal controls, and IT governance.	Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. Huawei Cloud's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
176.7	3. IT Controls Implementation.	c. IT controls implementation. BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1） Information security; 2） Project management/development and acquisition and change management; 3） IT operations; 4） IT outsourcing/Vendor management; 5） Electronic banking, Electronic payments, Electronic money and other Electronic products and services.	Huawei Cloud has established a comprehensive IT risk system based on international and industrial standards such as ISO27001, ISO20000, and CSA STAR, covering information security, privacy protection, business continuity management, IT service management and other fields. Huawei Cloud is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers.
176.7	3. IT Controls Implementation.	d. IT Outsourcing/Vendor Management Program. BSIs outsourcing IT services should have a comprehensive outsourcing risk management process which provide guidance on the following areas: 1） risk assessment; 2） selection of service providers; 3） contract review; and 4） monitoring of service providers.	Customers should establish processes and mechanisms for outsourcing management to ensure that risks related to outsourcing are properly identified and controlled. Huawei Cloud receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with risk assessment, contract review、performance monitoring and audit oversight activities initiated by customers.

9.2 IT Audit

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
5. IT	5.3.	Depending on the complexity	Huawei Cloud receives regular

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
AUDIT PHASES	Performance of Audit Work	of IT risk profile, IT auditors may perform all or a combination of any of the following IT audit procedures: a. IT General Controls Review. The following areas should be covered, among others: a) IT management and strategic planning; b) IT operations; c) Client/server architecture; d) Local and wide-area networks; e) Telecommunications; and f) Physical and information security. b. Application Systems Review - The purpose of this review is to identify, document, test and evaluate the application controls that are implemented to ensure the confidentiality, integrity and accuracy of the system processing and the related data. c. Technical Reviews - BSFI requires IT auditors to perform highly technical/ specialized reviews such as the conduct of periodic internal vulnerability assessment and penetration testing, computer forensics and review of emerging technologies, e.g., cloud computing, virtualization, mobile computing.	audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. To meet customers' compliance requirements, Huawei Cloud regularly conducts internal and third-party vulnerability scan, penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. On a quarterly basis, Huawei Cloud organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of Huawei Cloud. For all known security vulnerabilities, Huawei Cloud evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated. Huawei Cloud organizes internally or external third parties with certain qualifications to conduct penetration tests on all Huawei Cloud systems and applications every six months, and follow up and rectify the results of penetration tests. The penetration test report and follow-up would be verified by internal audits and external certification agencies.

9.3 Information Security

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.2. Physical and Environmental Protection. Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities. The BSFI should fully consider the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of its data centers. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could adversely affect the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator.	Huawei Cloud has established comprehensive physical security and environmental security protection measures, strategies, and procedures. Huawei Cloud data centers are located on suitable physical sites, as determined from solid site surveys. 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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers.
3. INFO	3.2. Security	3.2.3. Security Administration and Monitoring. A security	Huawei Cloud employees use unique IDs on the internal office

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
RMATION SECURITY STANDARDS	Controls Implementation	administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function. Management should employ the "least privilege" principle throughout IT operations.	network. Complete account lifecycle management regulations and processes have been established. Access to cloud services uses Identity and Access Management (IAM) to manage user access and permissions. 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. If the account user wants to use the account, the account administrator can initiate the authorization process and authorize the account by using a password or increasing the account's rights. The applicant and approver of the account cannot be the same person. In addition, 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. In addition, when Huawei Cloud O&M personnel access the Huawei Cloud management network to manage the system in a centralized manner, they must use a unique employee account. All user accounts are configured with strong password security policies, and their passwords are periodically changed to prevent brute force cracking. In addition, two-factor authentication, such as USB key and SmartCard, is used to authenticate Huawei Cloud O&M personnel. Employee

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			accounts are used to log in to VPNs and bastion hosts to implement in-depth audit of user logins. Moreover, Huawei Cloud uses Identity and Access Management (IAM) to provide user account management and identity authentication for enterprise-level organizations. When a customer enterprise has multiple users to operate resources collaboratively, IAM can be used to avoid sharing account keys with other users and assign minimum permissions to users as required. In addition, IAM can also be used to set login authentication policies, password policies, and access control lists (ACLs) to ensure user account security. Each Huawei Cloud customer has a unique user ID and provides multiple user identity authentication mechanisms, including account passwords and multi-factor authentication. In addition, IAM supports 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.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.4. Authentication and Access Control. Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfill one's duties. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization14	Huawei Cloud employees use unique IDs on the internal office network. Complete account lifecycle management regulations and processes have been established. Access to cloud services: IAM is used to control users' access and manage their rights. All O&M accounts, device accounts, and application accounts are managed in a unified manner to ensure the end-to-end management, including user

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		should be allowed to access confidential information and use system resources solely for legitimate purposes. The BSFI should have an effective process to manage user authentication and access control. Appropriate user authentication mechanism commensurate with the classification of information to be accessed should be selected. The grant, modification and removal of user access rights should be approved by the information owner prior to implementation. A user access re-certification process should be conducted periodically to ensure that user access rights remain appropriate and obsolete user accounts have been removed from the systems.	creation, authorization, authentication, and permission reclaiming. If the account user wants to use the account, the account administrator can initiate the authorization process and authorize the account by using a password or increasing the account's rights. The applicant and approver of the account cannot be the same person. In addition, 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. Huawei Cloud has established a periodic access permission review mechanism to ensure that operation logs are enabled to record access permission addition, change, and deletion operations. Security personnel periodically audit access permission change logs. If an uncleared exit account is found, the security personnel will ask the system administrator to clear it. The privileged account management system binds functional accounts or technical accounts for routine or 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 log in to the tenant console or resource instance only after obtaining the customer's authorization. Strong log audit is

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			supported on bastion hosts to ensure that O&M personnel can locate operations on target hosts.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.5. System Security. The following control procedures and baseline security requirements should be developed to safeguard operating systems， system software and databases，among others: • Clear definition of a set of access privilege for different groups of users and access to data and programs is controlled by appropriate methods of identification and authentication of users together with proper authorization; • Secure configuration of operating systems，system software，databases and servers to meet the intended uses with all unnecessary services and programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers; • Periodic checking of the integrity of static data（e.g. system parameters）to detect unauthorized changes; • Clear establishment of responsibilities to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified，assessed，tested and applied to the systems in a timely manner;	First, for access control, HUAWEI CLOUD's Identity and Access Management (IAM) provides identity authentication and cloud resource access control for customers. When O&M personnel access the HUAWEI CLOUD management network to centrally manage the system, they need to use employee IDs and two-factor authentication, such as USB keys and SmartCards. Employee accounts are used to log in to VPNs and bastion hosts to implement in-depth audit of user logins. 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. For security configuration, HUAWEI CLOUD hardens the security configurations of host operating systems, VMs, databases, and web application components, and allows customers to select appropriate security configurations based on their service requirements. For example, in terms of host security, the host OS uses Huawei Unified Virtualization Platform (UVP) to manage CPU, memory, and I/O resources in isolation. The host OS has been minimized and service security has been hardened. In terms of VM security, HUAWEI CLOUD provides security configurations such as image hardening, network and platform

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		• Adequate documentation of all configurations and settings of operating systems, system software, databases and servers; and • Adequate logging and monitoring of system and user activities to detect irregularities and logs are securely protected from manipulation.	isolation, IP/MAC spoofing control, and security groups. In addition, HUAWEI CLOUD uses an integrity check mechanism to ensure the integrity of system parameters. For example, at the VM OS layer, HUAWEI CLOUD Image Management Service (IMS) supports image integrity check. When a VM is created based on an image, the system automatically checks the image integrity to ensure that the created VM contains complete image content. In addition, a comprehensive change management procedure prevents HUAWEI CLOUD internal O&M personnel from changing system configuration parameters without authorization. In addition, HUAWEI CLOUD establishes a security patch management process for patch management and test environments to ensure that security patches are installed within the time limit specified in IT security standards. In addition, HUAWEI CLOUD has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services. Continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period. Huawei Cloud collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			data analysis system. The logs are kept for more than 180 days, and security measures are taken to prevent log tampering to enable compliance and backtracking of network security events. In addition, CTS provides operational records of cloud service resources for tenants, and many products and services also have log recording functions. Tenants can independently select log retention time according to their own needs to effectively support analysis of abnormal activities.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.6. Cyber Security. The BSFI must evaluate and implement appropriate controls relative to the complexity of its network. An effective approach to adequately secure system and data within the network involves the following, among others: ●Grouping of network servers, applications, data, and users into security domains （e.g., untrusted external networks, external service providers, or various internal user systems）; ●Establishment of appropriate access requirements within and between each security domain; ●Implementation of appropriate technological controls to meet access requirements consistently; and ●Monitoring of cross-domain access for security policy violations and anomalous activity.	Huawei Cloud divides a data center into multiple security zones based on service functions and network security risks to implement physical and logical control and isolation, improving the self-protection and fault tolerance capabilities of the network against intrusions and moles. There are five key security zones: DMZ, Public Service, POD-Point of Delivery, OBS-Object-Based Storage, and OM-Operations Management. To ensure that tenant services do not affect management operations and that devices, resources, and traffic are not monitored, Huawei Cloud divides the communication plane of its network into tenant data plane, service control plane, platform O&M plane, and baseboard management controller (BMC) based on different service functions, security risk levels, and permissions. Management Controller: management plane and data storage plane to ensure proper and secure distribution of network communication traffic related to different services, facilitating separation of duties. Huawei Cloud isolates data on the cloud by using the Virtual Private Cloud (VPC). VPC uses the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			network isolation technology to isolate tenants at Layer 3 networks. Tenants can fully control the construction and configuration of their own virtual networks. Connects VPCs to traditional data centers on tenants' intranets using VPNs or Direct Connects, implementing smooth migration of tenant applications and data from tenants' intranets to the cloud. On the other hand, the ACL and security group functions of the VPC are used to configure security and access rules on demand to meet tenants' fine-grained network isolation requirements.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.7. Remote Access. Controls over remote access are required to manage risk brought about by external connections to the BSI's network and computing resources.	Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. When O&M personnel access the Huawei Cloud management network to centrally manage the system, they need to use employee IDs and two-factor authentication, such as USB keys and SmartCards. Huawei Cloud administrators must pass two-factor authentication before accessing the management plane through bastion hosts. All operations are logged and sent to the centralized log audit system in a timely manner. Strong log audit is supported on bastion hosts to ensure that O&M personnel can locate operations on target hosts. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.8. Encryption. The BSFI should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include the following, among others: • Provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and • Adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.	Huawei Cloud formulates and implements 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 restoration, and destruction. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			backups to ensure key persistence.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.9. Malicious Code Prevention. The BSFI should provide protection against the risk of malicious code by implementing appropriate controls at the host and network level to prevent and detect malicious code, as well as engage in appropriate user education.	Huawei Cloud uses the IPS, WAF, antivirus software, and HIDS host intrusion detection system to manage vulnerabilities of system components and networks. IPS can detect and prevent potential network intrusions. WAF is deployed at the network border to protect application software from external attacks such as SQL injection, CSS, and CSRF. Antivirus software provides antivirus protection and firewalls in Windows systems. The HIDS host-based intrusion detection system protects ECSs and reduces the risk of account theft. It provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page tamper protection.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.10. Personnel Security, The BSFI should have a process to verify job application information on all new employees. Screening procedures, including verification and background checks, should be developed for recruitment of permanent and temporary IT staff, and contractors, particularly for sensitive IT-related jobs or access level. Management should obtain signed confidentiality, non-disclosure and authorized use agreements before granting new employees and contractors access to IT systems. Such agreements put all parties on notice that the BSFI owns its information, expects strict confidentiality, and prohibits information sharing outside legitimate	Huawei Cloud has developed policies and processes based on ISO27001. Before hiring an employee, if permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Simultaneously, to ensure orderly internal management and reduce the potential impact of personnel management risks on business continuity and security, Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including onboarding security review, on-thejob security training and enablement, onboarding qualifications management, and off boarding security review. The employment

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		business needs. All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate IS awareness training and regular updates in organizational policies and procedures relevant to their job function.	agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities. For external personnel, Huawei Cloud signs a non-disclosure agreement with them and conducts information security training, including information security responsibilities. Huawei Cloud continues security awareness training for employees during their employment. There is a special information security awareness training program for employees. This training includes but is not limited to, on-the-spot speeches and online video courses. Cybersecurity awareness courses are held periodically for employees to continually refresh their cybersecurity knowledge and help them understand relevant policies and systems. This way, they will be able to distinguish acceptable from unacceptable behavior, assume the responsibilities they have for any wrongdoing regardless of their intent, and abide by all company rules and legal requirements.
3. INFORMATION SECURITY STANDARDS	3.2. Security Controls Implementation	3.2.11. Systems Development, Acquisition and Maintenance. A framework should be in place describing the tasks and processes for development or acquisition of new systems, assignment and delineation of responsibilities and accountabilities for system deliverables and project milestones. User functional requirements, systems design and technical specifications and service performance expectations should be adequately documented and	Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. 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

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		approved at appropriate management levels. The BSFI's development, acquisition, and audit policies should include guidelines describing the involvement of internal audit and information security personnel in the development or acquisition activities as a means of independently verifying the adequacy of the control and security requirements as they are developed and implemented. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling should be clearly specified. The information and/or process owners should conform to the security requirements for each new system or system acquisition, accept tests against the requirements, and approve implementation of systems in the production environment. The BSFI should have an effective process to introduce application and system changes into its respective environments. The process should encompass development, implementation, and testing of changes to both internally developed software and acquired software. Weak procedures can corrupt applications and introduce new security vulnerabilities.	(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
3. INFO	3.3. Security	3.3.2. IS Incident Management. The BSFI	Huawei Cloud has developed a security incident management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
RMATION SECURITY STANDARDS	Process Monitoring and Updating	should establish incident response and reporting procedures to handle IS-related incidents. All employees, contractors and third party users shall be required to note and report any observed or suspected security weaknesses in systems. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Therefore, the BSFI should strictly control and monitor access to log files whether on the host or in a centralized logging facility. Where a follow-up action against a person or organization after an IS incident involves legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction.	mechanism, including a general security incident response plan and process, and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. Huawei Cloud formulates security incident grading rules and escalation rules, classifies security incidents based on the impact of security incidents on customers' services, initiates the customer notification process based on the security incident notification mechanism, and notifies customers of the incidents. When a serious security incident occurs, which has or may have severe impact on a large number of customers, Huawei Cloud can notify the customer of the incident information in the shortest time. At least include the incident description, measures taken by Huawei Cloud, and measures recommended to the customer. Once the incident is resolved, an incident report will be provided to the customer on a case-by-case basis. In addition, Huawei Cloud has dedicated personnel to keep in touch with industry organizations, risk and compliance organizations, local authorities, and regulators and establish contact points. Huawei Cloud uses a centralized log big data analysis system to collect management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. Logs are retained for more than 180 days. In addition, security measures are taken during log storage to prevent logs from being tampered with to ensure that cyber security event backtracking and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			compliance are supported. In addition, CTS records operations on cloud service resources for tenants. Many products and services also provide the log recording function. Tenants can select the log retention period based on their requirements to effectively support abnormal activity analysis.

9.4 Project Management/Development, Acquisition and Change Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
4. PROJECT PLANNING AND INITIATION	4.4	4.4. During the development and acquisition of new systems or other major IT projects, project plans should address issues such as — a） business requirements for resumption and recovery alternatives; b） information on back-up and storage; c） hardware and software requirements at recovery locations; d） BCP and documentation maintenance; e） disaster recovery testing; and f） staffing and facilities. Likewise, during maintenance, where there are changes to the operating environment, business continuity considerations should be included in the change control process and implementation phase.	Huawei Cloud complies with the ISO22301 international standard for business continuity management and has established a complete business continuity management system. Under this system framework, business impact analysis and risk assessment are performed periodically, and comprehensive recovery policies are formulated for key services that support continuous running of cloud services. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties. In addition, Huawei Cloud has developed a business continuity plan and disaster recovery plan and periodically tested them. The business continuity plan is designed for major disasters, such as earthquakes or public health crises, to ensure continuous running of cloud services and ensure the security of customers' services and data. The disaster recovery plan usually takes the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			cloud platform infrastructure and cloud services in a geographical location or region offline, simulates a disaster, and then performs system processing and transfer according to the disaster recovery plan to verify the service and operation functions of the faulty location. The test results are annotated and archived. for continuous improvement of the program. Huawei Cloud relies on the "two sites, three data centers" architecture of the data center cluster to implement DR and backup for data centers. Data centers are deployed around the world according to rules, and all data centers are running properly. In addition, the two sites serve as each other's DR centers. If a fault occurs in one site, the system automatically transfers customer applications and data out of the affected area under compliance policies, ensuring service continuity. Huawei Cloud also deploys a global load balancing scheduling center. Customers' applications are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. Huawei Cloud can replicate and store user data on multiple nodes in a data center. Once a single node is faulty, user data will not be lost and the system can automatically detect and recover. Data Center Interconnect (DCI) is implemented between different AZs in a single region through high-speed optical fibers, meeting basic requirements for cross-AZ data replication. Users can select DR replication services based on service requirements.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
5. SYSTEMS DEVELOPMENT	5.3	5.3. Programming standards should be designed to address issues such as the selection of programming languages and tools, the layout or format of scripted code, interoperability between systems, and the naming conventions of code routines and program libraries. These will enhance the BSFI's ability to decrease coding defects and increase the security, reliability, and maintainability of application programs.	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.
6. SYSTEM ACQUISITION	6.1	6.1. Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. A proper software selection analysis should be conducted to ensure that user and business requirements are met. In particular， the process should involve detailed evaluation of the software package and its supplier （e.g. its financial condition， reputation and technical capabilities）. If financial stability is in doubt，alternatives should be developed to reduce the adverse impact from loss of a vendor's service.	Customers should conduct due diligence prior to selecting a service provider, particularly with regard to governance, risk and compliance management mechanisms. (1)Financial strength: Huawei Cloud is Huawei's service brand. Since its launch in 2017, Huawei Cloud has been developing rapidly and its revenue has maintained a strong growth trend. (2)Business reputation: As always, Huawei Cloud adheres to the customer-centric principle, making more and more customers choose Huawei Cloud. Huawei Cloud has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			industries. Apart from Chinese mainland, Huawei Cloud was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. (3)Technical ability: Huawei Cloud provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. Huawei Cloud has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), Huawei Cloud AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, Huawei Cloud has created a new multicomputing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value.
6. SYSTEM ACQUISITION	6.2	6.2. The contract agreement between the BSFI and vendor should be legally binding. The BSFI should ensure all contract agreements outline all expected service levels and are properly executed to protect its interest. It is also important to ensure that vendor technicians and third-party consultants are subjected to at least, or preferably more stringent policies and controls compared to the in-house staff. In the case where contract personnel are employed, written contracts should also be in effect.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			To comply with customer requirements, Huawei Cloud has developed related processes to ensure that services can be provided to customers in a secure and compliant manner. If permitted by applicable laws, Huawei Cloud will conduct background checks on employees and external personnel before hiring them based on the confidentiality of the assets that can be accessed. Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers, including on-boarding security review, on-the-job security training and enablement, on-boarding qualifications management, and off-boarding security review. The employment agreement signed by the employee and the company contains a confidentiality clause, which clearly states the employee's information security responsibilities.
7. CHANGE MANAGEMENT	7.1-7.5	7.1 The change management procedures should be formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement is obtained from all related parties. 7.2 The change manage process should include the following: • Classification and prioritization of changes and determination of the impact of changes;	Huawei Cloud has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of Huawei Cloud Change Committee. Huawei Cloud has established formal internal testing and acceptance measures to ensure that only appropriate and authorized

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		• Roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel; • Program version controls and audit trails; • Scheduling, tracking, monitoring and implementation of changes to minimize business disruption; • Process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and • Post implementation verification of the changes made (e.g. by checking the versions of major amendments). 7.3. Requested changes should be screened before acceptance to determine alternate methods of making the changes, the cost of changes and time requirements for programming activity. System analysts should assess the impact and validity of the proposed changes and all critical change requests should be set as priority. 7.4. The actual cause that led to the request for change should be identified and adequately documented. Formal reports on analysis for problems raised and status of	changes are released to the production environment. Before the change goes live, 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 goes live 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.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		change requests (including closed and outstanding) should be reported to senior management on a periodic basis. 7.5. Audit trail of all change requests should be maintained. Programmers' activities should be controlled and monitored, and all jobs assigned should also be closely monitored against target completion dates.	
7. CHANGE MANAGEMENT	7.6-7.7	7.6. To enable unforeseen problems to be addressed in a timely and controlled manner, the BSFI should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data-related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day). 7.7. Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible, if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment.	Huawei Cloud has also developed a standardized emergency change management process. If emergency changes affect users, they will communicate with users in advance by announcement, mail, telephone, conference, or other means according to the prescribed time limit. If the emergency changes do not meet the prescribed notice time limit, the changes will be upgraded to Huawei Cloud senior leadership, and users will be notified promptly after the changes are implemented. Emergency changes are recorded. The old version and data of the program are retained before the changes are executed. The changes are guaranteed to proceed smoothly through two-person operation to minimize the impact on the production environment.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.	
7. CHANGE MANAGEMENT	7.8	7.8. Management should ensure that vendors permitted remote access to network resources are properly authorized. System logs showing activity on the system should be reviewed to ensure that unauthorized remote access has not taken place. Management may institute time of day restrictions for remote access，to limit the duration of time a user can access the network remotely （e.g. only during business hours）	Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
13. DISPOSAL	13.1	13.1. The BSFI may sometimes need to remove surplus or obsolete hardware, software, or data. Primary tasks include the transfer, archiving, or destruction of data records. Management should transfer data from production systems in a planned and controlled manner that includes appropriate backup and testing procedures. The BSFI should maintain archived repository of data in accordance with applicable record retention requirements and system documentation to facilitate reinstallation of a system into production, when necessary. Management should destroy data by overwriting old information	During the destruction of customer content data, Huawei Cloud deletes the specified data and all copies of the data. 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.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		or degaussing (demagnetizing) disks and tapes.	
14. ROLE OF AUDIT, INFORMATION SECURITY AND QUALITY ASSURANCE OFFICERS	14.2	14.2 Information Security. The BSFI should ensure that systems are developed, acquired and maintained with appropriate security controls. To do this, management should ensure that — a) systems are developed and implemented with necessary security features enabled and based on established security control requirements; b) software is trustworthy by implementing appropriate controls in the different project phases; and c) appropriate configuration management and change control processes exist, including an effective patch management process. Management should establish security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access, damage or other threats.	For the security of the development process, Huawei Cloud manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. Huawei Cloud has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. Huawei Cloud 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. In addition, Huawei Cloud has developed change management regulations and change processes. Different change types must comply with different change

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			management processes. Each change must be reviewed in multiple phases. 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. Huawei Cloud establishes a security patch management process to ensure that security patches are installed within the time limit specified in IT security standards. In addition, Huawei Cloud has developed a vulnerability management mechanism to ensure timely emergency response to security vulnerabilities of cloud platforms and cloud services. Continuously optimize the default security configurations of cloud platforms and products, apply patches or patches within the specified period, place patches in the R&D phase before patch installation, and flexibly simplify the security patch deployment period.

9.5 IT Operations

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3. IT OPERATIONS STANDARDS	3.1	3.1 Technology Inventory. BSFI management should perform and maintain an inventory of all its IT resources, recognize interdependencies of these systems and understand how these systems support the associated business lines. Management should ensure the inventory is updated on an on-going basis to reflect the BSFI's IT environment at any point in time.	Huawei Cloud uses the CAM asset management system to monitor the inventory and maintenance status of information assets recorded on the asset management platform, classify, monitor, and manage information assets, and generate an asset list. Huawei Cloud assigns an owner to each asset. Huawei Cloud has developed 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. Ensure that the company's assets are properly protected and shared.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.1. Environmental Controls. Management should configure the UPS to provide sufficient electricity within milliseconds to power equipment until there is an orderly shutdown or transition to the back-up generator. The back-up generator should generate sufficient power to meet the requirements of mission	Huawei Cloud has established comprehensive physical security and environmental security protection measures, strategies, and procedures. During the design, construction, and operation stages, the data centers have proper physical zoning and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		critical IT and environmental support systems. Similarly, IT operations centers should have independent telecommunication feeds from different vendors. Management should physically secure these cables to avoid accidental or malicious disconnection or severing. In addition, management should document wiring strategies and organize cables with labels or color codes to facilitate easy troubleshooting, repair, and upgrade. Every operations center should have adequate heating, ventilation, and air conditioning（HVAC）systems. Operations centers should be equipped with water detectors under raised flooring to alert management of leaks that may not be readily visible. Management should also consider installing floor drains to prevent water from collecting beneath raised floors or under valuable computer equipment. A variety of strategies are available for fire suppression. Lastly, Management should consider using video surveillance and recording equipment in all or parts of the facility to monitor activity and deter theft. Management should also use inventory labels, bar codes, and logging procedures to control the inventory of critical and valuable equipment.	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, security measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental security of Huawei Cloud data centers For physical security, Huawei Cloud imposes further requirements on equipment room location selection, access control, and security measures. When choosing a location for a Huawei Cloud data center, Huawei Cloud factors in the risks of potential natural disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a Huawei Cloud data center. Site

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water, and telecommunication circuits. 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. Huawei Cloud data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. For environment security, Huawei Cloud has further requirements on electrical security, temperature and humidity control, fire control, routine monitoring, water supply and drainage, and Anti-static control. For electrical security, Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud data centers employ a multi-level security 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. For 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. For 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. For 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 security hazards and ensures smooth operation of all data center equipment. For 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			the data center equipment, especially computer information systems. For 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.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.3. Change Management& Control. Complex BSFIs should have a change management policy that defines what constitutes a "change" and establishes minimum standards governing the change process. Simple BSFIs may successfully operate with less formality, but should still have written change management policies and procedures.	Huawei Cloud has formulated management regulations and change procedures for change management, before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. Changes can be released only after achieving the approval of Huawei Cloud Change Committee.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.4. Patch Management. Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Management should develop a process for managing version control of operating and application software to ensure implementation of the latest	Huawei Cloud uses the OSM work order system platform to configure the OS, release patches, and upgrade the OS. Before launching a cloud service product, the cloud service team needs to perform virus scanning and integrity check on the service release package (including the patch package). In addition, Huawei Cloud has established a security

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		releases. Management should also maintain a record of the versions in place and should regularly monitor the Internet and other resources for bulletins about product enhancements, security issues, patches or upgrades, or other problems with the current versions of the software.	vulnerability management process, assigns vulnerability administrators and related security roles to be responsible for vulnerability assessment, requires regular security critical patches to reduce vulnerability risks, and specifies vulnerability rating, responsibility allocation, and vulnerability handling requirements. In addition, Huawei Cloud has established a dedicated vulnerability response team to promptly assess and analyze the causes and threat levels of vulnerabilities, develop remedial measures, and evaluate the feasibility and effectiveness of the remedial measures.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.6. Network Management Controls. Network standards, design, diagrams and operating procedures should be formally documented, kept updated, communicated to all relevant network staff and reviewed periodically. Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimized by automatic re-routing of communications through alternate routes should critical nodes or links fail. The network should be monitored on a continuous basis to reduce the likelihood of network traffic overload and detect network intrusions. Powerful network analysis and monitoring tools, such as protocol analyzers, network scanning and sniffer tools, are normally used for	To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage （e.g. viewing of unencrypted sensitive information）. The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.	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, which will be covered in more detail throughout the rest of this chapter and the following chapters of the white paper. Huawei Cloud deploys Anti-DDoS devices, IPS devices, and web application firewalls at the network boundary to protect the boundary. Anti-DDoS devices can detect DDoS attacks, and IPS has the ability to analyze and block real-time network traffic, and can prevent exceptions. Protocol attacks, brute force attacks, port/vulnerability scanning, virus/Trojan horses, exploits targeting vulnerabilities and other intrusion behaviors. External firewalls can deal with external types of attacks, such as SQL injection, cross-site scripting attacks, and component vulnerabilities. Huawei Cloud strictly protects these border protection tools to prevent unauthorized use.
3. IT OPERATIONS STANDAR	3.3	3.3.2.7. Disposal of Media. Management should have procedures for the destruction and disposal of media containing	Huawei Cloud uses equipment containing storage media to be managed by a special

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
DS		sensitive information. These procedures should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Furthermore, disposal procedures should recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since data can be recovered, additional disposal techniques should be applied to remove sensitive information.	person, who will format it after use. When the storage medium storing the company's confidential information is scrapped, a special person shall ensure that the information stored on it is cleared and cannot be recovered. The treatment methods include degaussing, physical destruction or low-level formatting. When a physical disk needs to be decommissioned, Huawei Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, Huawei Cloud adheres industry standard practices and keeps a complete data deletion activity log for chain of custody and audit purposes.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.9. Event/Problem Management. Management should ensure appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day IT operations. The event/problem management process should be communicated and readily available to all IT operations personnel. Management should ensure it trains all operations personnel to act appropriately during significant events. Employees should also receive training to understand event response escalation procedures.	Huawei Cloud has developed a comprehensive event management process that adheres to the "four fast" principle (e.g. fast discovery, fast demarcation, fast isolation, and fast recovery). Events are responded to systematically according to the impact of the event on customers and the network as a whole. The event is recorded and tracked in the work order system to ensure that the event can be solved as root cause analysis is carried out. The incident management process is communicated to the relevant personnel to ensure that the personnel

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			perform the correct steps when an incident occurs.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.12. Systems and Data Back-up. The BSFI should back-up and store its data and program files in a secure off-site location to allow restoration of systems, applications. Written standards should document back-up methodologies，delineate responsibilities of appropriate personnel，and ensure uniform performance throughout the institution. Management should maintain inventories of back-up media stored off-site and periodically perform physical inventories to ensure all required back up materials are available.	User data can be replicated and stored on multiple nodes in Huawei Cloud data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery. Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. The Huawei Cloud security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			When significant changes take place in the organization and environment of Huawei Cloud, the effectiveness of business continuity level would also be tested.
3. IT OPERATIONS STANDARDS	3.3	3.3.2.13. Systems Reliability, Availability and Recoverability. • System Availability. BSFIs should achieve high systems availability（or near zero system downtime） for critical systems which is associated with maintaining adequate capacity, reliable performance， fast response time， scalability and swift recovery capability. Built-in redundancies for single points of failure should be developed and contingency plans should be tested so that business and operating disruptions can be minimized. • Technology Recovery Plan. BSFI should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. In formulating an effective recovery plan， scenario analysis should be included to identify and address various types of contingency scenarios. Scenarios such as major system outages which may be caused by system faults， hardware malfunction, operating errors or security incidents as well as a total inaccessibility of the primary data center should be considered. • Alternate sites for technology recovery The BSFI should make	1) System Availability. Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers" data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance, ensuring business continuity. Huawei Cloud has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure. Users can and should take full advantage of all these

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		arrangements for alternate and recovery sites for their business functions and technology in the event the business premises， key infrastructure and systems supporting critical business functions become unavailable. A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site.The recovery facility should be at a distance that would protect it from damage from any incident occurring at the primary site. • Disaster Recovery Testing. The BSFI should always adopt pre-determined recovery actions that have been tested and endorsed by management. The effectiveness of recovery requirements and the ability of BSFI's personnel in executing or following the necessary emergency and recovery procedures should be tested and validated at least annually. Various scenarios which include total shutdown or inaccessibility of the primary data center， as well as component failure at the individual system or application cluster level should be included in disaster recovery tests. Inter-dependencies between and among critical systems should be included in the tests. BSFIs whose networks and systems are linked to specific service providers and vendors， should consider conducting bilateral or multilateral recovery testing.	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). 2) Technology Recovery Plan. Huawei Cloud standardizes the emergency response process, formulates an emergency response plan, conducts emergency drills and tests periodically, and continuously optimizes the emergency response mechanism. Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP. 3) Alternate sites for technology recovery. Huawei Cloud has

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of Huawei Cloud Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. Huawei Cloud has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. 4) Disaster Recovery Testing. Huawei Cloud develops a business continuity plan and disaster recovery plan and periodically tests them. The Huawei Cloud security drill team regularly develops policies for different product types. (including basic services, operation centers, data centers, and overall organizations) and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			drills in different scenarios to maintain the effectiveness of the continuity plan.
3. IT OPERATIONS STANDARDS	3.4	3.4.1. Service Level Agreement (SLA). BSFI Management of IT functions should formulate an SLA with business units which will measure the effectiveness and efficiency of delivering IT services.	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation.
3. IT OPERATIONS STANDARDS	3.4. Risk Monitoring	3.4.3. Performance Monitoring. The BSFI should implement a process to ensure that the performance of IT systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable problems to be identified and corrected before they affect system performance. Monitoring and reporting also support proactive systems management that can help the BSFI position itself to meet its current needs and plan for periods of growth, mergers, or expansion of products and services. BSFI Management should also conduct performance monitoring for outsourced IT solutions as part of a comprehensive vendor	Huawei Cloud provides the online Huawei Cloud User Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed offline contract templates, which can be customized based on customer requirements. The audit and supervision rights of the customer and its regulatory agencies on Huawei Cloud will be specified in the agreement signed with the customer based on actual conditions. In addition, Huawei Cloud will provide dedicated personnel to actively cooperate with customers'

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		management program. Reports from service providers should include performance metrics, and identify the root causes of problems. Where service providers are subject to SLAs, management should ensure the provider complies with identified action plans, remuneration, or performance penalties.	monitoring and audit requirements on Huawei Cloud and provide performance reports required by customers. Huawei Cloud provides the CES. Cloud Eye Service (CES) is a comprehensive monitoring platform for Elastic Cloud Servers, bandwidth, and other resources. CES monitors alarms, notifications, and custom reports and diagrams in real time, giving the user a precise understanding of the status of service resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.

9.6 IT Outsourcing / Vendor Management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
3.IT OUTSOURCING /VENDOR RISK MANAGEMENT PROGRAM	3.1 Risk Assessment	3.1 Risk Assessment. Prior to entering into an outsourcing plan, the BSFI should clearly define the business requirements for the functions or activities to be outsourced, assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced，	Customer should conduct a risk assessment of its outsourced business and its preferred service provider to identify potential risks. Huawei Cloud will assign dedicated personnel to respond to customer requirements and provide related materials. In addition, Huawei Cloud has developed a comprehensive information security risk management mechanism and regularly conducts risk

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		the capability of the technology service provider（TSP） and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSFI.	assessment and compliance review to ensure secure and stable running of the Huawei Cloud environment. Huawei Cloud has established a supplier selection and monitoring system to manage suppliers' compliance with Huawei Cloud requirements and contract obligations through due diligence before contract signing and periodic evaluation after contract signing.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.2 Service Provider Selection	3.2 Service Provider Selection. Before selecting a service provide, the BSFI should perform appropriate due diligence of the provider's financial soundness，reputation, managerial skills, technical capabilities，operational capability and capacity in relation to the services to be outsourced.	Customers should conduct due diligence prior to selecting a service provider, particularly with regard to governance, risk and compliance management mechanisms. (1) Financial soundness. Huawei Cloud is Huawei's service brand. Since its launch in 2017, Huawei Cloud has been developing rapidly and its revenue has maintained a strong growth trend. (2). Reputation. As always, Huawei Cloud adheres to the customer-centric principle, making more and more customers choose Huawei Cloud. Huawei Cloud has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, Huawei Cloud was launched in Hong Kong (China), Russia, Thailand, South

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Africa and Singapore in succession. (3). Managerial skills. Huawei Cloud inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, Huawei Cloud can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. (4). Technical capabilities. Huawei Cloud provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. Huawei Cloud has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), Huawei Cloud AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, Huawei Cloud has created a new multi-computing cloud

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. (5). Operational capability. Huawei Cloud follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. Huawei Cloud regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.3 Outsourcing Contracts	3.3 The contract is the legally binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance， reliability， security， confidentiality and reporting. The BSFI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services.	Huawei Cloud provides the Huawei Cloud User Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level provided by Huawei Cloud, and the customer's audit rights and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of financial institutions. Huawei Cloud may modify or terminate the service or modify or remove the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		Agreements should have clauses setting out the rules and limitations on subcontracting. To provide accountability， it may be beneficial for the BSFI to include a provision specifying that the contracting service provider shall remain fully responsible with respect to parts of the services which were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors. An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies.	functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. Huawei Cloud will also assign dedicated personnel to cooperate with the customer in reviewing the contract and provide relevant materials. Huawei Cloud has established a comprehensive supplier management mechanism. It strictly manages the security of outsourcers and outsourced personnel, and regularly audits and evaluates suppliers' security. Huawei Cloud transfers customers' security requirements in contracts to suppliers to ensure that the products and services provided by suppliers can meet the security requirements of Huawei Cloud customers. In addition, Huawei Cloud will notify customers in a timely manner when important suppliers change based on customer requirements.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.4 Service Level Agreement（SLA）	3.4. Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability for the outsourced activity. Management should closely monitor the service provider's compliance with key SLA	Huawei Cloud provides the Huawei Cloud Customer Agreement and Huawei Cloud Service Level Agreement, which specify the service content and service level, and responsibilities of Huawei Cloud. In addition, Huawei Cloud has developed an offline contract template, which can be customized

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		provision on the following aspects, among others: ●Availability and timeliness of services; ●Confidentiality and integrity of data; ●Change control; ●Security standards compliance, including vulnerability and penetration management; ●Business continuity compliance; and ●Help desk support. SLAs addressing business continuity should measure the service provider's contractual responsibility for backup, record retention, data protection, and maintenance and testing of disaster recovery and contingency plans. Neither contracts nor SLAs should contain any extraordinary provisions that would exempt the service provider from implementing its contingency plans（outsourcing contracts should include clauses that discuss unforeseen events for which the BSFI would not be able to adequately prepare）.	based on the requirements of customer. Customer's audit and supervision rights in Huawei Cloud will be committed in the agreement signed with the Huawei Cloud according to the situation.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5 Ongoing Monitoring	3.5.1. Monitoring Program. As outsourcing relationships and interdependencies increase in materiality and complexity，the BS1 needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract. The program should employ	Financial institutions should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. Huawei Cloud will assign dedicated personnel to actively respond to the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity, particularly the following: ●contract/SLA performance; ●material problems encountered by the service provider which may impact the BSFI; ●financial condition and risk profile; and ●business continuity plan, the results of testing thereof and the scope for improving it.	requirements of financial institutions and provide related materials. In addition, Huawei Cloud has established a supplier selection and monitoring system to manage suppliers' compliance with Huawei Cloud requirements and contract obligations through due diligence before contract signing and periodic evaluation after contract signing.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5 Ongoing Monitoring	3.5.3. General Control Environment of the Service Provider. The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSFI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.	Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. Huawei Cloud provides Identity and Access Management (IAM) for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication and performs access control and rights management for users Huawei Cloud does not allow O&M personnel to access customers' systems and data without authorization. Huawei Cloud adopts strict security O&M regulations and processes to ensure remote O&M security with customer authorization. Centralized O&M management and auditing is achieved through VPNs and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.5 Ongoing Monitoring	3.6 Business Continuity Planning Consideration. The BSFI should integrate the provider's BCP into its own plan， communicate functions to the appropriate personnel， and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.	Huawei Cloud provides the high availability infrastructure, data redundancy and backup. Customers can rely on the multi-region and multi-AZ architecture of Huawei Cloud data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world based on rules. Customers can use two sites as disaster recovery centers for each other. If one site s faulty, the system automatically transfers customer applications and data out of he affected area when compliance policies are met, ensuring service continuity. To provide customers with continuous and stable cloud services, Huawei Cloud has developed a business continuity management system that meets its own business characteristics and has obtained the IS0 22301 certification. Huawei Cloud has a formal business continuity plan (BCP) and DR plan (DRP) as well, and conducts BCP drills and

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			DRP tests periodically to ensure continued operations of Huawei Cloud services in the event of a disaster, and the emergency response plan complies with the current organizational and IT environments, and continuously optimize the emergency response mechanism.
3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM	3.7	The outsourcing agreement should explicitly provide a clause allowing Bangko Sentral and BSFIs' internal and external auditors to review the operations and controls of the service provider as they relate to the outsourced activity.	The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual situation. Huawei Cloud will comply with the requirements specified in the agreements signed with BSFIs and assign dedicated personnel to actively cooperate with BSFIs and financial transaction entities to supervise and supervise the audit and supervision of Huawei Cloud.
4. EMERGING OUTSOURCING MODELS	4.4	BSIs should be fully aware of the unique attributes and risks associated with cloud computing, particularly in the following areas: ●Legal and Regulatory Compliance; ●Governance and Risk Management; ●Due Diligence; ●Vendor Management/Performance and Conformance; ●Security and Privacy; ●Data Ownership and Data Location and Retrieval; ●Business Continuity	Before customers outsource services such as data processing, data storage, and cloud computing, they must verify the capabilities of the service provider, including Legal and Regulatory Compliance; Governance and Risk Management; Due Diligence; Vendor Management/Performance and Conformance; Security and Privacy; Data security and Business Continuity Planning. In addition, Huawei Cloud receives audits from professional third-party audit organizations every

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		Planning.	year and provides dedicated personnel to actively respond to and cooperate with audit activities initiated by customers. In addition, Huawei Cloud has established a supplier selection and monitoring system to manage suppliers' compliance with Huawei Cloud requirements and contract obligations through due diligence before contract signing and periodic evaluation after contract signing. As a cloud service provider, Huawei Cloud has the following aspects: 1) Compliance with applicable laws and regulations: The development of Huawei Cloud business follows Huawei's strategy of "one policy for one country/ region, one policy for one customer", and on the basis of compliance with the security regulations and industry supervision requirements of the country or region where the customer is located. Huawei Cloud not only leverages and adopts excellent security practices from throughout the industry but also complies with all applicable country, and/regions, security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, Huawei Cloud continues to build and mature in areas such as our security related

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to customers. Huawei Cloud will also openly and cooperatively tackle cloud security challenges standing should-to-shoulder with customers and partners as well as relevant governments in order to support the security requirements of customers 2) Governance and risk management. Huawei Cloud inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, Huawei Cloud can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. 3) Due diligence and vender management. Huawei Cloud has established a supplier selection and supervision system, through due diligence before signing the contract and regular evaluation to manage the

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			supplier's compliance with the specific requirements and contract obligations of Huawei Cloud. Huawei Cloud will assign dedicated personnel to actively respond to the requirements of customer and provide related materials. Customers should ensure that their selected service providers can provide services in accordance with the contract and SLA. Huawei Cloud has developed an offline contract template, which can be customized based on the requirements of FIs. Huawei Cloud may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise. 4) Security and Privacy. Huawei Cloud has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. Huawei Cloud has obtained many authoritative security and privacy protection certificates in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on Huawei Cloud. Requirements for obtaining third-party audit reports can

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			be specified in the agreement signed by the customer based on the actual situation. 5) Data security. Data security refers to the comprehensive protection of users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. Huawei Cloud attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. Huawei Cloud will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, Huawei Cloud will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. 6) Business continuity planning. Huawei Cloud has obtained the certification of the ISO22301 business continuity management

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			system standard, established a business continuity management system internally, and formulated a business continuity plan, which contains the strategies and processes of natural disasters, accident disasters, information technology risks and other emergencies.
4. EMERGING OUTSOURCING MODELS	4.5	4.5. Adoption of community and hybrid cloud deployment models may also be allowed with prior Bangko Sentral approval, subject to the following: ●Compliance with existing Bangko Sentral rules and regulations on outsourcing;. ●Implementation of more robust risk management systems and controls required for these types of arrangements; ●Bangko Sentral may be allowed to perform onsite validation prior to implementing the cloud computing arrangement/s.	Huawei Cloud will identify relevant regulatory requirements and comply with its rules and regulations on outsourcing. BSFIs should establish a risk assessment framework to regularly assess the security of their technology infrastructure, including risks associated with outsourcing arrangements. Huawei Cloud will cooperate with customers in risk assessment as needed. Huawei Cloud has developed a comprehensive information security risk management mechanism, and periodically conducts risk assessment and compliance review to ensure secure and stable running of Huawei Cloud's cloud environment. Meanwhile, Huawei Cloud will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			situation.

9.7 Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
4. RISK MANAGEMENT CONTROLS	4.1	4.1.7. Infrastructure and Security Monitoring. The BSFI should establish an appropriate operating environment that supports and protects systems on e-services. It should proactively monitor systems and infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. The BSFI should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-services systems, servers, databases, and applications.	Huawei Cloud provides infrastructure for customers and regards infrastructure security as the core component of building a multi-dimensional full-stack cloud security protection system. It provides multi-layer security protection in terms of physical environment, network, platform, application program interface, and data. Huawei Cloud builds a secure infrastructure foundation so that tenants can access the cloud with confidence and use secure Huawei Cloud services to focus on business development. Huawei Cloud uses the situational awareness analysis system to correlate alarm logs of various security devices and perform unified analysis to quickly and comprehensively identify attacks that have occurred and predict threats that have not occurred. Supports multiple threat analysis models and algorithms, and uses threat intelligence and security consulting to accurately identify attacks. In addition, the system evaluates Huawei

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			Cloud security status in real time, analyzes potential risks, and provides warnings based on threat intelligence to prevent attacks. In addition, the Huawei Cloud log big data analysis system can quickly collect, process, and analyze massive logs in real time. It can interconnect with third-party security information and event management (SIEM) systems, such as ArcSight and Splunk.
4. RISK MANAGEMENT CONTROLS	4.1	4.1.9. Audit Trail. The BSFI should ensure that comprehensive logs are maintained to record all critical e-services transactions to help establish a clear audit trail and promote employee and user accountability. Audit logs should be protected against unauthorized manipulation and retained for a reasonable period (e.g. three months) to facilitate any fraud investigation and any dispute resolution if necessary.	Huawei Cloud's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. In addition, Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days.
4. RISK	4.2.	4.2.3. Incident Response	Huawei Cloud has developed

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
MANAGEMENT CONTROLS	Administrative and Management Controls	and Management. The BSFI should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-services during or outside office hours. A communication strategy should be developed to adequately address the reported concerns and an incident response team	a security incident management mechanism, including a general security incident response plan and process. and continuously optimize the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. In addition, Huawei Cloud has a 7 x 24 professional security incident response team and corresponding security expert resource pool to handle security incidents. Huawei Cloud formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the financial institution business, and initiates a process to notify financial institutions of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple financial institutions, Huawei Cloud can promptly notify financial institutions of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by Huawei Cloud and the measures recommended for financial institutions. After the incident is resolved, the incident report will be provided to the financial institutions according to the specific situation.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
4. RISK MANAGEMENT CONTROLS	4.3. Consumer Protection	4.3.1. Customer Privacy and Confidentiality. The BSFI should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the institution is providing electronic products and services. Misuse or unauthorized disclosure of confidential customer data exposes the entity to both legal and reputation risk. To meet these challenges concerning the preservation of privacy of customer information, the BSFI should make reasonable endeavours to ensure that: • The BSI's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-services; • Customers are made aware of the BSI's privacy policies and relevant privacy issues concerning use of e-services; • Customers may decline ("opt out") from permitting the BSFIto share with a third party for cross-marketing purposes any information about the customer's personal needs, interests, financial position or banking activity; and • Customer data are not used for purposes	In each country and region, Huawei Cloud has dedicated legal affairs and privacy protection personnel to help Huawei Cloud activities meet applicable privacy laws and regulations. Customers have full control over their content data and act as responsible parties. Customers shall ensure that personal information is collected for specific, explicit, and legitimate purposes, inform data subjects of the purpose of collecting personal information, and obtain data subjects' consent. Huawei Cloud does not touch customer content data, nor does it know for what purpose it was collected.

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
		beyond which they are specifically allowed or for purposes beyond which customers have authorized. The BSI's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.	
5.INDEPENDENT ASSESSMENT	5.3	5.3. Subsequent to an initial independent assessment, the BSFI should conduct risk assessment at least every two years or when there are substantial changes to determine if further independent assessment should be required and the frequency and scope of such independent assessment. Any substantial changes to the risk profile of the services being provided, significant modifications of the network infrastructure and applications, material system vulnerabilities or major security breaches are to be taken into consideration in the risk assessment.	Huawei Cloud has established information security risk management regulations and developed information security risk assessment methods to identify risks from multiple dimensions, and judge the possibility of risks based on the completeness of security policies, security technologies, and security audits. Huawei Cloud is responsible for any major changes during service provisioning. Information security risk assessment will be performed periodically based on actual requirements. Risk assessment covers all aspects of information security. Based on the confidentiality, integrity, and availability of business processes and assets, major modifications to network infrastructure and applications, major system vulnerabilities, or major security vulnerabilities of Huawei Cloud are considered, and risk rating is performed. Formally document the assessment and develop a risk management plan. Huawei Cloud regularly hires independent third

No.	Control Domain	Specific Control Requirements	Huawei Cloud Response
			parties to provide external audit and verification services. These evaluators perform regular security assessment and compliance audits or checks. (e.g. SOC, ISO standards, PCI DSS audit) to assess the security, integrity, confidentiality, and availability of information and resources for an independent assessment of risk management content/processes. Huawei Cloud will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's audit and supervision rights on Huawei Cloud will be promised in the agreement signed with the customer based on the actual situation.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

10 Conclusion

This whitepaper describes how Huawei Cloud provides cloud services that meet regulatory requirements of the financial industry in Philippines and shows that Huawei Cloud complies with key regulatory requirements issued by the Bangko Sentral ng Pilipinas. This aims to help customers learn more about Huawei Cloud's compliance status with Philippine regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this whitepaper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of the Philippine financial industry on Huawei Cloud, and assists customer to better identify security responsibilities together with Huawei Cloud.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

11 Version History

Date	Version	Description
June 2022	1.0	First release
August 2024	1.1	Regular update

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.