# HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in Malaysia

**Issue** 2.1

**Date** 2024-07-17

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

### Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Contents



# 1 Overview

## 1.1 Background and Purpose of Publication

With the more prevalent use of technology in the provision of financial services, there is a need for financial institutions (FIs) to strengthen their technology resilience against operational disruptions to maintain confidence in the financial system. The growing sophistication of cyber threats also calls for the increased vigilance and capability of FIs to respond to emerging threats. Critically, this should ensure the continuous availability of essential financial services to customers and adequate protection of customer data. To regulate the application of Information Technology (IT) in the financial industry, Bank Negara Malaysia (BNM) and Securities Commission Malaysia (SC) published a series of regulatory requirements and guidelines, covering technology risk management, IT outsourcing management, customer information protection and business continuity management for FIs operating in Malaysia.

HUAWEI CLOUD, as a cloud service provider, is committed not only to help FIs meeting local regulatory requirements, but also to continuously provide them with cloud services and business operating environments meeting FIs' standards. This whitepaper sets out details regarding how HUAWEI CLOUD assists FIs operating in Malaysia to meet regulatory requirements when providing cloud services.

## 1.2 Introduction of Applicable Financial Regulatory Requirements in Malaysia

**Bank Negara Malaysia (BNM)**

- Risk Management in Technology (RMiT)**:** This policy document sets out Bank Negara Malaysia's requirements with regard to FIs' management of technology risk. In complying with these requirements, a FI shall have regard to the size and complexity of its operations. Accordingly, larger and more complex FIs are expected to demonstrate risk management practices and controls that are commensurate with the increased technology risk exposure of the institution. In addition, all FIs shall observe minimum prescribed standards in this document to prevent the exploitation of weak links in interconnected networks and systems that may cause detriment to other FIs and the wider financial system.
- Outsourcing**:** This policy document sets out the scope of arrangements relevant to the outsourcing policy, and Bank Negara Malaysia's requirements and expectations on FIs to

maintain appropriate internal governance and outsourcing risk frameworks, including those relevant to the protection of data confidentiality. The requirements also serve to ensure the FIs' continued ability to carry out effective supervisory oversight over FIs in relation to their outsourced activities.

- Management of Customer Information and Permitted Disclosures**:** This policy document sets out Bank Negara Malaysia's requirements and expectations with regard to financial service providers'(FSP) measures and controls in handling customer information, throughout the information lifecycle, covering collection, storage, use, transmission, sharing, disclosure and disposal of customer information.
- Guidelines on Data Management and Management Information System Framework for Development Financial Institutions**:** This policy document sets out high level guiding principles on sound data management and management information system (MIS) practices that FIs should observe when developing internal data management capabilities. FIs should structure and implement data and management information systems in a manner that is consistent with the principles set out in this document and appropriate to each FI's specific business needs.
- Business Continuity Management**:** The purpose of this policy document is to facilitate the development and implementation of a robust BCM framework, policies and processes by financial institutions which are integrated with their overall risk appetite and reinforce sound risk management practices; strengthen the capacity and preparedness of financial institutions to respond and recover from operational disruptions; and preserve the continuity of critical business functions and essential services within a specified timeframe in the event of an operational disruption.
- Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMIT) Policy Document (Exposure Draft)**:** This exposure draft set out the guidelines for the assessment of common key risks and considerations of control measures when financial institutions adopt cloud services. The proposed expectations serve as supplementary guidance to the Risk Management in Technology (RMiT) policy document to strengthen financial institutions' cloud risk management capabilities.

**Securities Commission Malaysia (SC)**

- Guidelines on Management of Cyber Risk**:** This policy document sets out Securities Commission Malaysia's requirements with regard to FIs' management of cyber risk. These requirements will help FIs improve their cyber risk management capabilities and ensure their cyber security.
- Guiding Principles on Business Continuity**:** The objective of this document is to guide the FIs on minimum standards where entities are encouraged to adopt based on the nature, size and complexity of their business operations. The overall intended outcomes of the principles are to ensure timely continuation of critical services and the fulfilment of business obligations in the event of disruptions and ultimately with the objectives to mitigate or manage any possible wider systemic risk implications to the Malaysian capital market.

*****Remarks***: *The above regulatory requirements issued by BNM are applicable to FIs such as banks and insurance companies. The above regulatory requirements issued by SC are applicable to FIs such as Bursa Malaysia, Capital Markets Services License (CMSL) holders, registered persons and self-regulatory organizations under securities laws. For specific applicable objects, please refer to the original regulatory requirements.*

# 1.3 Definitions

- **HUAWEI CLOUD**

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

- **Service provider**

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

- **Cyber Resilience**

  The ability of people, processes, IT systems, applications, platforms or infrastructures to withstand adverse cyber events.

- **Central bank of Malaysia (The Bank)**

  Bank Negara Malaysia (BNM).

- **Business Continuity Plan**

  Refers to a comprehensive action plan that documents the processes, procedures, systems and resources necessary to resume and restore the operations and services of a financial institution in the event of a disruption.

- **Crisis Management Plan**

  Refers to a comprehensive action plan that documents the procedures and processes to support decision making by the crisis management team (CMT) in the event of a crisis. It includes criteria for activating the BCP and disaster recovery plan (DRP).

- **Disaster Recovery Plan (DRP)**

  Refers to a comprehensive action plan that documents the procedures and processes that are necessary to recover and restore information technology systems, applications and data of a financial institution in the event of a disruption.

- **Critical Business Functions (CBF)**

  Refers to business functions undertaken by a financial institution, where the failure or discontinuance of such business functions is likely to–

  (a) critically impact the financial institution financially or non-financially; and

  (b) disrupt the provision of essential services to its customers.

- **Maximum Tolerable Downtime (MTD)**

  Refers to a comprehensive action plan that documents the procedures and processes that are necessary to recover and restore information technology systems, applications and data of a financial institution in the event of a disruption.

- **Recovery Time Objective (RTO)**

  Refers to the timeframe required for systems and applications of a financial institution to be recovered and operationally ready to support its critical business functions after a disruption. A recovery time objective has the following two components:

  (a) the duration of time from the disruption to the activation of the BCP; and

  (b) the duration of time from the activation of the BCP to the recovery of the business operations.

# 2 HUAWEI CLOUD's 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 |

| Certification | Description |
|---|---|
| | third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology. |
| PCI DSS Certification | Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict FI certification in the world. |
| CSA STAR Gold Certification | CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity. |
| International Common Criteria EAL 3+ Certification | Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide. |
| ISO 27018:2014 | ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management. |
| 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 an authoritative professional certification organization. Huawei cloud data centers have obtained the M&O certification issued by Uptime Institute. The |

| Certification | Description |
|---|---|
| | M&O certification symbolizes that HUAWEI CLOUD data center O&M management has been leading in the world. |
| NIST CSF (Cybersecurity Framework) | NIST CSF consists of three parts: standards, guidelines, and best practices for managing cyber security risks. The core content of the framework can be summarized as the classic IPDRR capability model, five capabilities: Identify, Protect, Detect, Response, and Recovery. |
| PCI 3DS | The PCI 3DS standard is designed to protect the 3DS environment that performs specific 3DS functions or stores 3DS data, and supports 3DS implementation. PCI 3DS evaluates the 3D protocol execution environment, including the access control server, directory server, or 3DS server function. and system components, such as firewalls, virtual servers, network devices, and applications, that are required in and connected to the 3D execution environment; In addition, the process, process, and personnel management of the 3D protocol execution environment are evaluated. |

**Regional standard certification**

| Certification | Description |
|---|---|
| Classified Cybersecurity Protection of China's Ministry of Public Security | Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4. |
| Singapore MTCS Level 3 Certification | 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) | 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) | This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking. |

| Certification | Description |
| --- | --- |
| ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) | ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates. |
| TRUCS | Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China. |
| Cloud Service Security Certification - Cyberspace Administration of China (CAC) | This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization. |

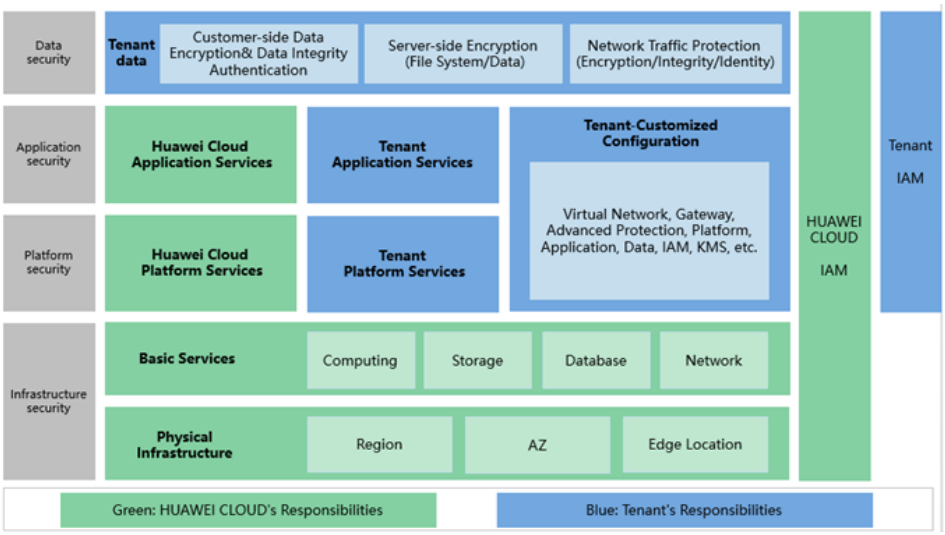
For more information on HUAWEI CLOUD security compliance and downloading relevant compliance certificate, please refer to the official website of HUAWEI CLOUD "Trust Center -Compliance".

# 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 tenant and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenants to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the tenant and HUAWEI CLOUD:

**Figure 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.

**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 tenants and HUAWEI CLOUD, please refer to the HUAWEI CLOUD Security White Paper released by HUAWEI CLOUD.

# 4 HUAWEI CLOUD Global Infrastructure

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

# 5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Risk Management in Technology

BNM released *Risk Management in Technology* on June 19, 2020. This policy set FIs' technology risk management requirements from the perspectives of governance, technology risk management, technology operations management, cyber security management, technology audit, internal awareness and training, and notification for technology. Among them, the domain of technology operations management includes requirements for system development and acquisition, cryptography, data center resilience, network resilience, third party service provider management, cloud services, access control, etc. The domain of cyber security management includes requirements for cyber security operations, data loss prevention, cyber response and recovery, etc.

When FIs are seeking to comply with the requirements provided in *Risk Management in Technology*, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following contents summarize the compliance requirements related to cloud service providers in *Risk Management in Technology*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

## 5.1 Technology Operations Management

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| System Development and Acquisition-10.5, 10.6, 10.7, 10.8, 10.10, | 10.5 A FI must establish clear risk management policies and practices for the key phases of the system development life cycle (SDLC) encompassing system design, development, testing, deployment, | Customers should establish a security development management mechanism, and establish clear risk management policies and | As a cloud service provider:<br>**(1)** Huawei's development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| 10.12, 10.13, and 10.14 | change management, maintenance and decommissioning. Such policies and practices must also embed security and relevant enterprise architecture considerations into the SDLC to ensure confidentiality, integrity and availability of data.<br>10.6 A FI is encouraged to deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to support more secure systems development.<br>10.7 A FI shall consider the need for diversity in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.<br>10.8 A FI must establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, the FI must ensure proper authorization procedures and adequate measures to | measures for the SDLC encompassing system design, development, testing, deployment, change management. The management mechanism is not limited to the use of automated tools, the development of secure coding standards, code review, isolation of the test environment and the production environment, etc., and the managing changes through formal procedures shall be taken into consideration as well. | 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.<br>HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, applicable 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 safety design library and complete the corresponding safety 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 the safety of products and services.<br>**(2)** HUAWEI CLOUD strictly complies with the security coding specifications of various programming languages issued by Huawei. Static code analysis tools are used for routine checks, and the resulting data is entered in the cloud service tool chain to evaluate the quality of coding. Before all cloud services are released, static code analysis alarms must be cleared to effectively reduce the security issues related to coding when online.<br>**(3)** HUAWEI CLOUD takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services to meet the security |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | prevent their unauthorized disclosure are in place.<br>10.10 A FI must ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure code is secure and was developed in line with recognized coding practices prior to introducing any system changes.<br>10.12 A FI shall physically segregate the production environment from the development and testing environment for critical systems. Where a FI is relying on a cloud environment, the FI shall ensure that these environments are not running on the same virtual host.<br>10.13 A FI must establish appropriate procedures to independently review and approve system changes. The FI must also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimize any business disruption.<br>10.14 Where a FI's IT systems are managed by third party service providers, the FI shall ensure, including through contractual obligations, that the third party service | | requirement of the released cloud services. Testing is conducted in a test environment, isolated from the production environment, and avoids the use of production data for testing. If production data is used for testing, it must be desensitized, and data cleaning is required after use.<br>**(4)** To meet customer compliance requirements, HUAWEI CLOUD has formulated a standardized change management process. Any change to the environment will take place only by orderly management process. 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, that the change committee can clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. In addition, HUAWEI CLOUD has formulated more fine-grained change operation standards to guide the implementation, tracking, and verification of the change to achieve the expected purpose of the change.<br>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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | providers provide sufficient notice to the FI before any changes are undertaken that may impact the IT systems. | | 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. After the implementation, a designated person will verify it to help the change achieves its desired purpose. |
| Cryptography - 10.16, 19.19, and 10.20 | 10.16 A FI must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information.<br>10.19 A FI must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols must be based on recognized international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation must be | Customers should establish cryptography management policy. When customers use encryption to protect data, they should consider using industry-recognized encryption algorithms and key management mechanisms, and use the certificate of the specialized certification authorities to manage the storage and transmission of the key.<br>Huawei Cloud provides the **Data Encryption Workshop (DEW)** for customers. The DEW key management | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which supports data security on the cloud. DEW adopts the layered key management mechanism. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to help user to meet the requirements of data security compliance. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with customers' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys. See section 6.8.2 Data Encryption Workshop (DEW) of **HUAWEI CLOUD Security White Paper** for more information.<br>**(2)** Currently, services including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEM).<br>10.20 A FI shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognized certificate authorities. The FI must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. | 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. | provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms.<br>**(3)** For data in transmission, when customers provide Web site services through the Internet, they can use certificate management services provided by the HUAWEI CLOUD United Global Well-known Certificate Service Provider. By applying for and configuring certificates for Web sites, the trusted identity authentication of Web sites and secure transmission based on encryption protocols are realized. |
| Data Center Resilience - Data Center Infrastructure-10.21-10.24 | 10.21 A FI must specify the resilience and availability objectives of its data centers which are aligned with its business needs. The network infrastructure must be designed to be resilient, secure and scalable. Potential data center failures or disruptions must not significantly degrade the delivery of its financial services or impede its internal operations. | Customers should establish resilient and highly available data centers which are aligned with their business needs. The security and scalability of network infrastructure, independent space and physical | As a cloud service provider, HUAWEI CLOUD will cooperate with customers to meet regulatory requirements from the following perspectives:<br>**(1)** HUAWEI CLOUD data centers comply with Class A standard of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standard of *TIA-942 Telecommunications Infrastructure Standard for Data Centers.* 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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | 10.22 A FI must ensure production data centers are concurrently maintainable. This includes ensuring that production data centers have redundant capacity components and distribution paths serving the computer equipment.<br>10.23 In addition to the requirement in paragraph 10.22 large FIs are also required to ensure recovery data centers are concurrently maintainable.<br>10.24 A FI shall host critical systems in a dedicated space intended for production data center usage. The dedicated space must be physically secured from unauthorized access and is not located in a disaster-prone area. A FI must also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centers, including hardware components, electrical utility, thermal management and data center infrastructure. A FI must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults | security of key systems, redundancy of infrastructure and hardware equipment, continuous monitoring of the environment and resources, etc. should be considered to prevent serious impacts of its services or internal operations from data center's failures or disruptions. | 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, appropriate and sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers. See section 5.1 Physical and Environmental Security of **HUAWEI CLOUD Security White Paper** for more information.<br>**(2)** 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. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | and indicators of potential issues. | | |
| Data Center Resilience - Data Center Operations - 10.26, 10.27, and 10.30 | 10.26 A FI must ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth.<br>10.27 A FI must establish real-time monitoring mechanisms to track capacity utilization and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.<br>10.30 A FI must also maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup media must be stored in an environmentally secure and access-controlled backup site. | Customers should establish performance monitoring and capacity planning mechanisms, plan and manage the capacity of their IT basic resources based on business development, and continuously monitor the performance of key systems. In addition, customers should establish a backup management mechanism to back up key business data, operating systems, and application software.<br>Customers can use the versioning function of **Object Storage Service (OBS)**, **Volume Backup Service (VBS)**, and **Cloud Server Backup** | In order to cooperate with customers to meet regulatory requirements:<br>**(1) Cloud Eye Service (CES)** provides users with a robust monitoring platform for **Elastic Cloud Server (ECS)**, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.<br>**(2)** HUAWEI CLOUD has formulated a standard capacity management and resource forecasting procedure to manage Huawei's cloud capacity as-a-whole and improve the availability of Huawei's cloud resources. HUAWEI CLOUD resource utilization is monitored daily. Input from all parties provides ongoing predictions for future resource requirements, and resource expansion schemes are formulated to meet these requirements. Business capacity and performance bottlenecks are analyzed and evaluated. When resources reach a preset threshold, a warning is issued, and further solutions are adopted to avoid the impact on the system performance of the user cloud service.<br>**(3)** HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | **Service (CSBS)** to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also back up data through HUAWEI CLOUD's data backup archiving service to ensure that data will not be lost in the event of a disaster. | |
| Network Resilience - 10.33, 10.34, 10.35, 10.36, 10.38, and 10.39 | 10.33 A FI must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.<br>10.34 A FI must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.<br>10.35 A FI must establish real-time network bandwidth monitoring processes | Customers should establish a reliable and scalable enterprise network, including the deployment of redundant network lines, the establishment of network performance monitoring, network channel encryption, network equipment log storage, | As a cloud service provider:<br>**(1)** HUAWEI CLOUD responses that it is responsible for securing development, configuration, deployment, and operation of various cloud technologies, and it is responsible for the security of operation, maintenance and operation of the cloud services it provides. Therefore, in the initial phase, HUAWEI CLOUD will strictly implement the corresponding control measures to support that the HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration.<br>**(2)** Customers can rely on HUAWEI |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | and corresponding network service resilience metrics to flag any over utilization of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.<br>10.36 A FI must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.<br>10.38 A FI must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.<br>10.39 A FI must implement appropriate safeguards to minimize the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the FI from other entities within the group. | appropriate network isolation and other measures.<br>In view of the scenario of hybrid cloud deployment and global layout of customer services, customers can use the **Virtual Private Network (VPN)**, **Direct Connect (DC)**, **Cloud Connect (CC)**, and other services provided by HUAWEI CLOUD to realize business interconnection and data transmission security between different regions.<br>HUAWEI CLOUD's **Cloud Trace Service (CTS)** provides operating records of cloud service resources for users to query, for auditing and backtrack use. There are | CLOUD's data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N+1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.<br>**(3)** HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent.<br>**(4)** The VPN service uses Huawei's professional equipment and VPN on Internet based on IKE and IPsec protocols. It constructs a secure and reliable encryption transmission channel between a local data center and HUAWEI CLOUD VPCs in different areas. Direct Connect is based on operators' various types of dedicated line network. It builds exclusive encrypted transmission channels between local data center and HUAWEI CLOUD VPC. Physical isolation between customer dedicated lines meets higher security and stability requirements. Cloud Connect can quickly establish a private communication network |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within HUAWEI's cloud system.<br>Customers can use the **Virtual Private Cloud (VPC)**, **Elastic Load Balance (ELB)** to network isolation and load balancing between different regions. | between multiple local data centers and multiple cloud VPCs, support the interconnection of cross-cloud VPCs, and greatly improve the security and speed of global expansion of customer services.<br>**(5)** CTS can merge records into event files on a regular basis and move these to an OBS bucket for storage, making logs highly available over a long period of time and at a low cost. At the same time, HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information.<br>**(6)** The VPC service provided by HUAWEI CLOUD for customers can create a private network environment for users, and realize complete isolation of different users in a three-tier network. Users have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation. The ELB automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Third Party Service Provider Management - 10.42, 10.43, 10.46, 10.47, and 10.48 | 10.42 A FI must conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the third party service provider's capabilities in managing the following specific risks:<br>(a) data leakage such as unauthorized disclosure of customer and counterparty information;<br>(b) service disruption including capacity performance;<br>(c) processing errors;<br>(d) physical security breaches;<br>(e) cyber threats;<br>(f) over-reliance on key personnel;<br>(g) mishandling of confidential information pertaining to the FI or its customers in the course of transmission, processing or storage of such information;<br>(h) concentration risk.<br>10.43 A FI must establish service-level agreements (SLA) when engaging third party service providers. At a minimum, the SLA | Customers should conduct due diligence on service providers' competency, system infrastructure and financial viability and capabilities in managing risks before selecting them.<br>Customers shall sign a legally-binding agreement with the service provider, and stipulate the terms of cooperation in auditing, confidentiality, business continuity arrangements, notifications, service termination, etc. to protect the customer's rights and interests and meet regulatory requirements.<br>When the service agreement terminates, customers can migrate content data from HUAWEI | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** HUAWEI CLOUD will arrange a responsible personnel to actively cooperate with due diligence requirements initiated by customers. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.<br>**(2)** HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. As the case may be, the auditing and supervision rights of customers and regulatory authorities will be stipulated in the agreement signed with the customer.<br>**(3)** HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so customers can seek help with methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.<br>To meet the requirement for fast response, HUAWEI CLOUD has developed a complete event management process. Events are prioritized and different processing time limits are defined according to |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | shall contain the following:<br>(a) access rights for the regulator and any party appointed by the FI to examine any activity or entity of the FI.<br>(b) requirements for the service provider to provide sufficient prior notice to FIs of any sub-contracting which is substantial;<br>(c) a written undertaking by the service provider on compliance with secrecy provisions under relevant legislation;<br>(d) arrangements for disaster recovery and backup capability, where applicable;<br>(e) critical system availability; and<br>(f) arrangements to secure business continuity in the event of exit or termination of the service provider.<br>10.46 A FI must ensure data residing in third party service providers are recoverable in a timely manner. The FI shall ensure clearly defined arrangements with the third party service provider are in place to facilitate the FI's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber- | CLOUD through **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD, such as migrating to local data center. | the impact and scope of each event. HUAWEI CLOUD will respond to and resolve the event within a specified time limit according to the priority of the event, to minimize the impact of the event on cloud service customers.<br>**(4)** HUAWEI CLOUD will not use customer data for commercial monetization and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the applicable laws and regulations or the binding orders of the government institutions. HUAWEI CLOUD conforms to the data protection principles described in *the Personal Data Protection Act* (PDPA) of Malaysia. In addition, HUAWEI CLOUD service products and components have planned and implemented appropriate isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all take customer data isolation as an important feature.<br>**(5)** HUAWEI CLOUD infrastructure has high availability. HUAWEI CLOUD has developed a sound internal process to continuous monitoring, regular maintenance and regular testing of infrastructure operation, to minimize the impact of system failures on customers. Customers can rely on HUAWEI CLOUD's data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are deployed around the world so customers will have mutual disaster data backup centers in case of |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | incident.<br>10.47 A FI must ensure the storage of its data is at least logically segregated from the other clients of the third party service provider. There shall be proper controls over and periodic review of the access provided to authorized users.<br>10.48 A FI must ensure any critical system hosted by third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service provider. | | disasters. In the event of one failure in an area, the system automatically transfers customer applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N+1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. HUAWEI CLOUD has set up a multiple position backup mechanism for key positions supporting cloud services. |
| Cloud Services -10.51 and 10.53 | 10.51 A FI is required to consult the Bank prior to the use of public cloud for critical systems. The FI is expected to demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in the following areas:<br>(b) the availability of independent, internationally recognized certifications of the | Customers should consult the Bank prior to the use of public cloud for critical systems and evaluate the security qualifications of cloud service providers. In addition, customers should also develop data protection measures to prevent illegal access to data on cloud | As a cloud service provider:<br>**(1)** HUAWEI CLOUD has received a number of international and industry security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, CSA STAR, etc.<br>HUAWEI CLOUD follows 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.<br>**(2)** HUAWEI CLOUD will not use |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | cloud service providers, at a minimum, in the following areas:<br>(i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and<br>(ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit.<br>10.53 A FI must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | services.<br>Huawei Cloud provides the **Data Encryption Workshop (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. | customer data for commercial monetization and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the applicable laws and regulations or the binding orders of the government institutions. HUAWEI CLOUD conforms to the data protection principles described in *the Personal Data Protection Act* (PDPA) of Malaysia. In addition, HUAWEI CLOUD service products and components have planned and implemented appropriate isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all take customer data isolation as an important feature.<br>**(3)** HUAWEI CLOUD services including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms.<br>**(4)** The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which supports data security on the cloud. DEW adopts the layered key management mechanism to facilitate the rotation of keys at all levels. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to help customers to meet |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | the requirements of data security compliance. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with customers' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys.<br>See section 6.8.2 Data Encryption Workshop (DEW) of **HUAWEI CLOUD Security White Paper** for more information. |
| Access Control -10.54, 10.56, 10.57, and 10.58 | 10.54 A FI must implement an appropriate access controls policy for the identification, authentication and authorization of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorized access to its technology systems.<br>10.56 A FI must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic | Customers should implement an appropriate access controls policy and adopt reliable authentication methods, such as multi-factor authentication . In addition, customers should review and update their password policies regularly to ensure the security of passwords.<br>Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and** | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** Each HUAWEI CLOUD customer has a unique user ID in HUAWEI CLOUD, and provides a variety of user authentication mechanisms.<br>• IAM supports the security administrators of customers to set up different password strategies and change cycles according to their needs to prevent users from using simple passwords or using fixed passwords for a long time, resulting in account leakage. In addition, IAM also supports customers' security administrators to set up login strategies to avoid users' passwords being violently cracked or to leak account information by visiting phishing pages.<br>• IAM supports multi-factor authentication mechanism at the same time. MFA is an optional security measure that enhances account security. If MFA is enabled, users who have completed password authentication will receive a one-time SMS authentication code that they must use for secondary |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).<br>10.57 A FI shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created.<br>10.58 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, FIs are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents. | **Access Management (IAM)**.<br>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. | authentication. MFA is used by default for changing important or sensitive account information such as passwords or mobile phone numbers.<br>• If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists.<br>**(2)** HUAWEI CLOUD has established a sound operation and maintenance account management mechanism. 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. User accounts are equipped with strong password security policies, and passwords are changed regularly to prevent violent decryption. In addition, two-factor authentication is used to authenticate cloud personnel, such as USB key, Smart Card and so on. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to fully manage user creation, authorization, and authentication to rights collection processes. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | different responsibilities in different positions are limited to access the equipment under their role. |
| Patch Management - 10.65 | A FI must establish a patch management framework which addresses among others the following requirements:<br>(a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches;<br>(b) conduct of compatibility testing for critical patches;<br>(c) specification of turnaround time for deploying patches according to the severity of the patches; and<br>(d) adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities. | Customers should establish an effective patch and vulnerability management mechanism to identify and conduct risk assessment of all technology assets, compatibility testing for critical patches, and formulate patch update cycle and patch repair workflow.<br>HUAWEI CLOUD **Image Management Service (IMS)** provides simple and convenient self-service management functions for images. Customers can manage their images through the IMS API or the management console. | As a cloud service provider:<br>**(1)** HUAWEI CLOUD staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to refer in deployment testing, troubleshooting, and other O&M activities.<br>**(2)** The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service model, the program ensures rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructures, platforms, applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and technical means. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | impact on customers' services. |

## 5.2 Cyber Security Management

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Cybersecurity Operations - 11.7-11.9 | 11.7 A FI must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure.<br>11.8 A FI must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large FIs, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems.<br>11.9 A FI must conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all | Customers should deploy effective tools to establish the monitoring of technical infrastructure, conduct vulnerability assessments on the network formation of critical systems quarterly, and conduct annual penetration testing mechanisms on the network infrastructure and critical systems.<br>HUAWEI CLOUD's **Cloud Trace Service (CTS)** provides operating records of cloud service resources for users to query, for auditing and backtrack use. | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** CTS inspects the log data sent by various services that ensures the data itself does not contain sensitive information. In the transmission phase, it guarantees the accuracy and comprehensiveness of log information transmission and preservation by means of identity authentication, format checking, whitelist checking and a one-way receiver system; In the storage phase, it adopts multiple backups according to Huawei's network security specifications and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. 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.<br>**(2)** The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | external-facing applications. The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A FI must engage suitably accredited penetration testers and service providers to perform this function. | There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within Huawei's cloud system. | model, the program ensures rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructures, platforms, applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and technical means. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on clients' services.<br>**(3)** HUAWEI CLOUD regularly conducts internal and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services. Together with partners, HUAWEI CLOUD has launched host intrusion detection, web application firewall, host vulnerability scanning, web page anti-tampering, and penetration test services, which enhance the security detection, correlation, and protection capabilities of HUAWEI CLOUD. |
| Distribu ted | A FI must ensure its technology systems | Customers should | In order to cooperate with customers to meet regulatory requirements: |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Denial of Service (DDoS)-11.13 | and infrastructure, including critical systems outsourced to or hosted by third party service providers, are adequately protected against all types of DDoS attacks (including volumetric, protocol and application layer attacks) through the following measures:<br>(a) subscribing to DDoS mitigation services, which include automatic 'clean pipe' services to filter and divert any potential malicious traffic away from the network bandwidth;<br>(b) regularly assessing the capability of the provider to expand network bandwidth on-demand including upstream provider capability, adequacy of the provider's incident response plan and its responsiveness to an attack; and<br>(c) implementing mechanisms to mitigate against Domain Name Server (DNS) based layer attacks. | establish anti-DDoS attack mechanism, purchasing anti-DDoS attack services, regularly assessing the capability of the provider to expand network bandwidth on-demand, implement measures to prevent DNS layer attacks.<br>HUAWEI CLOUD provides customers with two kinds of Anti-DDoS attack services: **Anti-DDoS** and **Advanced Anti-DDoS (AAD)**. | **(1)** Anti-DDoS is a traffic scrubbing service that protects resources such as Elastic Cloud Server and Elastic Load Balance instances from network and application layer distributed denial-of-service (DDoS) attacks. It notifies users of detected attacks instantly, ensures bandwidth availability as well as the stable and reliable running of services. AAD can be used to protect HUAWEI CLOUD and non-HUAWEI CLOUD hosts. User can change the DNS server or external service IP address to a high-defense IP address, thereby diverting traffic to the high-defense IP address for scrubbing malicious attack traffic. This mechanism ensures that important services are not interrupted.<br>**(2)** HUAWEI CLOUD Anti-DDoS attack services provide fine-grained DDoS mitigation capabilities to deal with the likes of Challenge Collapsar attacks and ping, SYN, UDP, HTTP, and DNS floods. Once a protection threshold is configured (based on the leased bandwidth and the business model), Anti-DDoS will notify the affected user and activate protection in the event of a DDoS attack.<br>**(3)** HUAWEI CLOUD Anti-DDoS attack services also leverages other HUAWEI CLOUD technologies to enhance its security capabilities: namely, the secure infrastructure and platform, secure network architecture, perimeter protection, virtual network isolation, API security, and log auditing. |
| Data Loss Prevention (DLP)-11.15 | A financial institution must design internal control procedures and implement appropriate technology in all applications and access points to enforce DLP policies and trigger any policy violations. The | Customers should establish a data leakage prevention mechanism and use appropriate technical means to | In order to ensure the safe processing of data on the cloud by customers, HUAWEI CLOUD provides layer-by-layer protection for all stages of the data life cycle:<br>**(1) Data creation**: HUAWEI CLOUD provides services on a regional basis, which is the storage location of customer content data. HUAWEI CLOUD will never |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | technology deployed must cover the following:<br>(a) data in-use – data being processed by IT resources;<br>(b) data in-motion – data being transmitted on the network; and<br>(c) data at-rest – data stored in storage mediums such as servers, backup media and databases. | prevent data leakage. The deployed technology should cover the data life cycle of data usage, data transmission, and data storage.<br>Huawei Cloud provides the **Data Encryption Workshop (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. | transfer customer content data across regions without authorization. Customers choose areas based on the principle of nearby access and applicable laws and regulations in different regions when customers use cloud services, so that customer content data is stored in the target location. When customers use cloud hard drives, object storage, cloud databases, container engines and other services, HUAWEI CLOUD uses different granular access control mechanisms such as volumes, buckets, database instances, and containers to enable customers to only access their own data.<br>**(2) Data storage**: Currently, **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which supports data security on the cloud.<br>**(3) Data usage**: HUAWEI CLOUD provides customers with services in data access control, security protection, and auditing to help them control data usage and transfer in a fine-grained manner.<br>For more information, please refer to Section 4.5 of "Whitepaper for HUAWEI CLOUD Data Security".<br>**(4) Data transmission**: When customers provide Web site services through the Internet, they can use the certificate management service provided by HUAWEI CLOUD in conjunction with world-renowned certificate service providers. By applying and configuring a certificate |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | for the Web site, the trusted identity authentication of the website and the secure transmission based on the encryption protocol are realized. For customer business hybrid cloud deployment and global layout scenarios, the virtual private network (VPN), cloud dedicated line service, cloud connection and other services provided by HUAWEI CLOUD can be used to achieve business interconnection and data transmission security between different regions.<br>**(5) Data archiving**: HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS**,** **Volume Backup Service (VBS)**, and **Cloud Server Backup Service (CSBS)** to back up in-cloud documents, disks, and servers. By integrating with data encryption services, backup data can also be encrypted and stored conveniently and quickly, effectively ensuring the security of backup data.<br>**(6) Data destroying**: If customers want to delete data or data needs to be deleted due to the expiration of a service, HUAWEI CLOUD will strictly follow applicable laws and regulations, as well as agreement with customers, delete the stored customer data in accordance with data destruction standards. |
| Security Operations Center (SOC)-11.17 | A FI must ensure its SOC, whether managed in-house or by third party service providers, has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the FI to detect anomalous user or network activities, flag potential breaches | Customer should establish SOC to detect user or network activities, identify breaches and establish the appropriate response. | As a cloud provider:<br>**(1)** HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the FI's reviews of its cybersecurity posture and strategy. | | information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. HUAWEI CLOUD also has a dedicated internal audit department that performs periodic audits on O&M activities. HUAWEI CLOUD log system based on big 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.<br>**(2)** HUAWEI CLOUD has built a appropriate, multi-layered full stack security framework with comprehensive perimeter defense. For example, layers of firewalls isolate networks by security zone, anti-DDoS quickly detects and protects against DDoS attacks, WAF detects and fends off web attacks close to real time, and IDS/IPS detects and blocks network attacks from the Internet in the real time while also monitoring for behavioral anomalies on the host.<br>See section 8.3 Security Logging & Event Management of **HUAWEI CLOUD Security White Paper** for more information. |
| Cyber Response and Recovery - 11.22-11.25 | 11.22 A FI must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the | Customers should establish cyber crisis management policies and procedures, establish and implement a | As a cloud service provider:<br>**(1)** HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | organization's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident.<br>11.23 A FI must establish and implement a comprehensive Cyber Incident Response Plan (CIRP).<br>11.24 A FI must ensure that relevant Cyber Emergency Response Team<br>(CERT) members are conversant with the incident response plan and handling procedures, and remain contactable at all times.<br>11.25 A FI must conduct an annual cyber drill exercise to test the effectiveness of its CIRP, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. | comprehensive Cyber Incident Response Plan (CIRP), and ensure that relevant CERT members are conversant with it. In addition, conduct an annual cyber drill exercise to test the effectiveness of its CIRP. | 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. 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. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD formulates the classification and escalation principles 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.<br>**(2)** HUAWEI CLOUD has formulated various specific contingency plans to deal with complex security risks in the cloud environment. Each year, HUAWEI CLOUD conducts contingency plan drills for major security risk scenarios |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | to quickly reduce potential security risks and ensure cyber resilience when such security incidents occur. HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes. |

# 5.3 Technology Audit

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Technology Audit - 12.5 | A FI must establish a technology audit plan that provides appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services. | Customers should establish a technology audit plan, and review critical technology services, third party service providers, material external system interfaces, etc. | As a cloud service provider, if a FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible person to actively cooperate with the audit. Customer's audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third party every year. |

# 5.4 Internal Awareness and Training

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Internal Awareness and Training -13.1-13.4 | 13.1 FI must provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles, and measure the effectiveness of its education and awareness programs. This cybersecurity awareness education must be conducted at least annually by the FI and must reflect the current cyber threat landscape.<br>13.2 A FI must provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent to effectively perform their roles and responsibilities.<br>13.3 In fulfilling the requirements under paragraph 13.2, a large FI shall ensure the staff working on day-to-day IT operations such as IT security, project management and cloud operations are also suitably certified.<br>13.4 A FI must provide its board members with regular | Customers should establish a cybersecurity training mechanism, provide adequate and regular security awareness training for all employees, and provide security risk management and technical training for professionals to ensure that the staff are competent to effectively perform their roles and responsibilities. | As a cloud service provider, to raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations, Huawei provides employee with security awareness training in three ways: company-wide awareness training, awareness promotion events, and the signing of Business Conduct Guidelines (BCG) commitment agreements. By utilizing industry best practices, Huawei has established a comprehensive cybersecurity training program, which implements security competency trainings for new hires as well as existing and newly-promoted employees. This program boosts employees' security competencies and improves employee capabilities of delivering to our customers secure products, services, and solutions that are compliant with all relevant laws and regulations. In order to streamline internal personnel management and to minimize any potential impact of personnel management on our business continuity and security, HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers. This program includes: on boarding security review, on the job security training and enablement, on boarding qualifications management, off boarding security review.<br>See section 4.4 Human Resource Management of **HUAWEI CLOUD Security White Paper** for more information. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | training and information on technology developments to enable the board to effectively discharge its oversight role. | | |

# 6 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Outsourcing

BNM released *Outsourcing* on October 23, 2019. This policy set FIs' outsourcing management requirements from the perspectives of responsibilities of the board and senior management, outsourcing process and management of risks, outsourcing outside Malaysia, outsourcing involving cloud services, approval for outsourcing arrangements, and submission of outsourcing plans. Among them, the domain of outsourcing process and management of risks includes requirements for assessment of service provider, outsourcing agreements, protection of data confidentiality, and business continuity planning.

When FIs are seeking to comply with the requirements provided in *Outsourcing*, 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 *Outsourcing*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

## 6.1 Outsourcing Process and Management of Risks

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Assessment of Service Provider -9.3 | A FI must conduct appropriate due diligence of a service provider at the point of considering all new arrangements, and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process must be commensurate with the materiality of the outsourced activity. | Customers should conduct appropriate due diligence of a service provider at the point of considering all new arrangements, or renewing or renegotiating existing arrangements, including | As a cloud service provider, HUAWEI CLOUD's performance in the aforesaid aspects is as follows:<br>**(1)Technical ability:** HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions based on its experience in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | The due diligence process must cover, at a minimum:<br>(a) capacity, capability, financial strength and business reputation;<br>(b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management;<br>(c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites;<br>(d) access rights of the FI and the Bank to the service provider;<br>(e) measures and processes to ensure data protection and confidentiality;<br>(f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement;<br>(i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document. | technical capabilities, financial resources, business reputation, risk management capabilities, location of outsourcing activities, data security, reliance on subcontractors, etc. | 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.<br>**(2)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. According to the *Market Share: IT Services, worldwide 2019* study released by Gartner, HUAWEI CLOUD ranked sixth in the global IaaS market and is one of the top three within China market, with a fastest growth rate up to 222.2% in the world.<br>**(3)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.<br>**(4)Operational capability:** HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | 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. 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.<br>**(5)Data center location:** Customers can use their own choice of data center when purchasing cloud services. HUAWEI CLOUD will follow the customer's choice. Without the customer's consent, HUAWEI CLOUD will not migrate customer content from the selected region, unless: (a) it must be migrated to comply with applicable laws and regulations or binding orders of government agencies; or (b) for technical services or for investigation of security incidents or investigating violations of contractual requirements.<br>**(6) Access rights of the FIs and regulatory authority**: Please refer "Outsourcing Agreement" in section 6.1 "Outsourcing Process and Management of Risks" of this |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | document.<br>**(7) Data security**: Please refer "Data Confidentiality Protection" in section 6.1 "Outsourcing Process and Management of Risks" of this document.<br>**(8) Subcontracting management** In order to cooperate with customers in exercising its supervision over service providers, the online **HUAWEI CLOUD Customer Agreement** divides the security responsibilities of cloud service customers and Huawei, while the **HUAWEI CLOUD Service Level Agreement** defines the level of services provided by HUAWEI CLOUD. In addition, HUAWEI CLOUD has also formulated an offline contract template. According to the specific requirements of the customer, it can stipulate that if HUAWEI CLOUD hires subcontractors, HUAWEI CLOUD shall notify the customer and be responsible for the subcontracted services. HUAWEI CLOUD has formulated supplier management mechanism, and has put forward security requirements from the supplier's products and the supplier's internal management. In addition, HUAWEI CLOUD conducts regular audits of suppliers, and network security agreements will be signed with suppliers involved in network security. During the service process, the quality of services will be continuously monitored and the performance of suppliers will be scored. Suppliers with poor security performance will be cooperatively downgraded.<br>**(9)Corporate culture and service policies suitable for FIs:** HUAWEI CLOUD defines product safety and functional |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | requirements according to customer business scenarios, applicable laws and regulations, regulatory requirements in product, service planning and design phases. Huawei implements these in R&D, and design phases to meet customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and Huawei's comprehensive cloud services. |
| Outsourcing Agreement -9.6 and 9.7 | 9.6 An outsourcing arrangement must be governed by a written agreement that is legally enforceable. The outsourcing agreement must, at a minimum, provide for the following: duration of the arrangement with date, responsibilities of the service provider, security control of service, data usage scope, service provider inspection, business continuity plan, notification obligation, breach clause, termination clause, etc.<br>9.7 The outsourcing agreement must also contain provisions which: (a) enable the Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity; (b) enable the Bank to conduct on-site supervision of the service provider where | Customer should sign a legally binding service agreement with the service provider and ensure the legality and suitability of the terms of the agreement. | To cooperate with customers to meet regulatory requirements, HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed according to the actual situation. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | the Bank deems necessary; (c) enable the Bank to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where the Bank deems necessary; and (d) allow the FI the right to modify or terminate the arrangement when the Bank issues a direction to the FI to that effect. | | |
| Protection of Data Confidentiality - 9.8 and 9.9 | 9.8 It is imperative that the FI satisfies itself that the level of security controls, governance, policies, and procedures at the service provider are robust to protect the security and confidentiality of information shared under the outsourcing arrangement.<br>9.9 A FI must ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, the FI must ensure that:<br>(d) where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are | Customers should use agreement restrictions, reviews, and other means to ensure the measure of security controls, governance, policies, and procedures at the service provider are robust and secure, and can effectively protect the security and confidentiality of information. | To meet regulatory requirements, HUAWEI CLOUD cooperates with the customers as the following:<br>**(1)** 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 safety regulations and industry supervision requirements of the country or region where the customer is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific 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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | comparable to Malaysia;<br>(e) where the service provider provides services to multiple clients, the FI's information must be segregated 18 from the information of other clients of the service provider;<br>(f) the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even after the arrangement has ceased; and<br>(g) information shared with the service provider is destroyed, rendered unusable, or returned to the FI in a timely and secure manner once the outsourcing arrangement ceases or is terminated. | | sustainable security infrastructure and services to our customers. We will also openly and cooperatively tackle cloud security challenges standing should-to-shoulder with our customers and partners as well as relevant governments in order to support the security requirements of our cloud users. 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.<br>**(2)** HUAWEI CLOUD will not use customer data for commercial monetization and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the applicable laws and regulations or the binding orders of the government institutions. HUAWEI CLOUD conforms to the data protection principles described in *the Personal Data Protection Act* (PDPA) of Malaysia.<br>**(3)** HUAWEI CLOUD service products and components have planned and implemented appropriate isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature.<br>**(4)** When the service agreement terminates, customers can migrate |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | content data from HUAWEI CLOUD through **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD, such as migrating to local data center.<br>Upon the confirmation of the destruction of customer data by the customers, HUAWEI CLOUD clears the specified data and all the copies. 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, so 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 so that data on the storage medium cannot be restored. |
| Business Continuity Planning -9.10, 9.13, and 9.14 | 9.10 A FI is responsible for ensuring that its Business continuity planning (BCP) consider any operational disruptions at, or failure of, the service provider.<br>9.13 A FI must, at all times, ensure that it has ready access to all its records and information at the service provider with respect to the outsourced activity which would be necessary for it to operate and meet its legal and regulatory obligations.<br>9.14 A FI must periodically test its own BCP and proactively seek assurance on the | Customers should ensure its BCP has considered any operational disruptions at, or failure of, the service provider and ensure that it has ready access to all its records and information at the service provider with respect to the outsourced activity. In addition, customer should periodically test its own BCP, and ensures that | To meet regulatory requirements, HUAWEI CLOUD cooperates with customers :<br>**(1)** To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response.<br>**(2)** HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | state of BCP preparedness of the service provider and where relevant, alternative service providers. The intensity and regularity of the BCP testing and assessments of BCP preparedness must be commensurate with the materiality of the outsourcing arrangement. In assessing this preparedness, the FI must, at a minimum:<br>(a) ensure that the back-up arrangements are available and ready to be operated when necessary;<br>(b) ensure that the service provider periodically tests its BCP and provides any test reports, including any identified deficiencies, that may affect the provision of the outsourced service and measures to address such deficiencies as soon as practicable; and<br>(c) for material outsourcing arrangements, participate in joint testing with the service provider to enable an end-to-end BCP test for these arrangements by the FI. | service providers test their business continuity plans and make continuous improvements. | specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation.<br>**(3)** 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.<br>**(4)** As a supplier of cloud service customers, HUAWEI CLOUD will actively cooperate with customer-initiated test requirements and help customers test the effectiveness of their BCPs.<br>HUAWEI CLOUD tests the BCPs and disaster recovery plans annually according to the requirements of the internal business continuity management system. All emergency response |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | personnel, including reserve personnel, need to participate. The tests include desktop exercises, functional exercises and full-scale exercises, in which high-risk scenarios are emphasized. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After the completion of the test, relevant personnel write the test report and summarize any problems found during the test. If the test results show problems with the BCPs, recovery strategy or emergency plan, the documents will be updated. |

# 6.2 Outsourcing Outside Malaysia

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Outsourcing Outside Malaysia -10.1-10.3 | 10.1 Outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia exposes a FI to additional risks (e.g. country risk). A FI should have in place appropriate controls and safeguards to manage these additional risks, having regard to social and political conditions, government policies, and legal and regulatory developments.<br>10.2 In conducting the due diligence process, a FI must ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the FI or service | When choosing foreign outsourced service providers, customers should conduct due diligence in advance to ensure that government policies, economic conditions, legal supervision and service capabilities of outsourced service providers meet the needs of customer | In order to cooperate with customers to meet regulatory requirements, HUAWEI CLOUD will arrange special personnel to actively cooperate with the customer during their due diligence. In addition, Huawei's cloud business follows Huawei's strategy of "one policy for one country/region, one policy for one customer" which complies with the safety regulations of the customer's country or region and the requirements of industry supervision. It also establishes and manages a highly trusted and sustainable security guarantee system towards the aspects of organization, process, norms, technology, compliance, |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | provider to implement appropriate responses to emerging risk events in a timely manner.<br>10.3 A FI must ensure that outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect:<br>(a) the FI's ability to effectively monitor the service provider and execute the institution's BCP;<br>(b) the FI's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and<br>(c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity. | business development and regulatory requirements. | ecology and other aspects that adheres to the best practices of the industry. In an open and transparent manner, we will work with relevant governments, customers and industry partners to meet the challenges of cloud security and support the security needs of customers in an all-round way. For more information, please refer to the relevant content of "Business Continuity Plan" in section 6.1 "Outsourcing Process and Management of Risks" of this document. |

# 6.3 Outsourcing Involving Cloud Services

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Outsourcing involving Cloud Services -11.3 and 11.4 | 11.3 In relation to a FI's ability to conduct audits and inspections on the cloud service provider and sub-contractors pursuant to paragraph 9.6(f), the FI may rely on third party certification and reports made available by the cloud service provider for the audit, provided | Customers should regularly review cloud service providers, or obtain third-party certification and reports. In addition, customers | In order to cooperate with customers to meet regulatory requirements, if an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible persons to actively cooperate regarding the audit. Customer's audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the HUAWEI CLOUD according to the |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit.<br>11.4 In relation to the testing of a cloud service provider's BCP pursuant to paragraph 9.6(i), a FI must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising from the BCP testing. | should also obtain information about business continuity management of the cloud service providers. | situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third party every year.<br>For more information about HUAWEI CLOUD's business continuity management, please refer to the relevant content of "Business Continuity Plan" in section 6.1 "Outsourcing Process and Management of Risks" of this document. |

# 7 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Management of Customer Information and Permitted Disclosures

BNM released issued *Management of Customer Information and Permitted Disclosures* on 21 October 2021 to replace the *Management of Customer Information and Permitted Disclosures* issued on 17 October 2017. This policy set FIs' customer information management requirements from the perspectives of board oversight, senior management, control environment, customer information breaches, and outsourced service provider and other domains. Among them, the domain of control environment includes requirements for risk assessment, policies and procedures, information and communication technology controls, access control, physical security, and independent review, etc.

When FIs are seeking to comply with the requirements provided in *Management of Customer Information and Permitted Disclosures*, 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 *Management of Customer Information and Permitted Disclosures*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

## 7.1 Control Environment

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Risk Assessment - 10.1 and 10.2 | 10.1 FSPs must identify potential threats and vulnerabilities that could result in theft, loss, misuse, or unauthorized access, modification or disclosure by whatever means. | Customers should identify potential security threats and vulnerabilities, and assess the likelihood that such threat and vulnerability, as | As a cloud service provider, HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of GB 50174 Code for Design of Electronic Information System Room and T3+ standard of TIA-942 Telecommunications |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | 10.2 FSPs must also assess the likelihood that such threat and vulnerability will materialize and the potential impact it will have on the FSP and its customers in the event a customer information breach occurs. | well as the potential impact caused by security incidents. | Infrastructure Standard for Data Centers. The HUAWEI CLOUD O&M team regularly carries out risk assessment on global data centers to ensure that data centers strictly implement access control, security measures, routine monitoring and audit, emergency response and other measures. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities, so that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third-party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers. |
| Policies and Procedures -10.6 and 10.11 | 10.6 FSPs must establish and have in place written policies and procedures to safeguard customer information, which covers collection, storage, use, transmission, sharing, disclosure and disposal of customer information.<br>10.11 FSPs must continually review their policies and procedures to ensure that they remain adequate, relevant and operate effectively in response to changes in the operating | Customers should formulate and implement data security policies and procedures to protect the entire life cycle of customer information. In addition, Customers should continually review their policies and procedures to ensure their adequacy and effectiveness. | To ensure the safe processing of data on the cloud by customers, HUAWEI CLOUD implements layer-by-layer protection at all phases of the data life cycle. For details, please refer to the relevant content of "Data Loss Prevention" in section 5.2 "Cyber Security Management" in this document. 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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | environment. | | activities every year to identify problems in the operation of the system each year and rectify them to continuously improve the management system. |
| Control Measures - Information and Communication Technology (ICT) Controls -10.12, 10.13, 10.20, and 10.21 | 10.12 FSPs must deploy preventive and detective ICT controls to prevent theft, loss, misuse or unauthorized access, modification or disclosure of customer information and to detect errors and irregularities when they occur.<br>10.13 FSPs must regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats.<br>10.20 FSPs must have in place mechanisms that create a strong deterrent effect against unauthorized disclosure by whatever means of customer information by staff.<br>10.21 Unauthorized disclosure may occur in many ways and forms such as staff taking photograph of documents or screens that contain customer information. The mechanisms referred to in paragraph 10.20 may include raising staff awareness on the disciplinary actions for unauthorized disclosure by whatever means, installing CCTV at | Customers should deploy preventive and detective ICT controls, regularly monitor the effectiveness of these controls, and establish an accountability mechanism for information disclosure.<br>Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**.<br>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 | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** HUAWEI CLOUD's **Identity and Access Management (IAM)** provides cloud resource access control for customers.With IAM, the customer administrator can manage user accounts and control the operation rights of these user accounts to the resources under the customer name; **Cloud Trace Service (CTS)** can provide customers with operational records of cloud service resources for users to query, audit and retrospective use. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within Huawei's cloud system.<br>HUAWEI CLOUD will not use customer data for commercial monetization and explicitly states in the user agreement that it will not access or use the user's content unless it provides the necessary services for the user or abides by the applicable laws and regulations or the binding orders of government organs. When internal operation and maintenance personnel access HUAWEI CLOUD<br>management network for centralized management of the system, they need to use two-factor authentication for identity authentication, such as USB key, Smart Card and so on. Employee account is used to log on VPN and Fortress Machine to realize the deep audit of user login. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | relevant areas, having an open office concept, encouraging whistleblowing in this respect, or restricting personal electronic devices at high risk areas like data centers, dealing rooms, call centers, etc. | location. | **(2)** Huawei has established a rigorous security responsibility system and implemented accountability measures against security violations. On the one hand, HUAWEI CLOUD carries out our responsibilities in accordance with the shared responsibility model and takes full responsibility for any security violation caused by HUAWEI CLOUD in order to minimize user business impact. On the other hand, HUAWEI CLOUD mandates that every employee be responsible for his/her actions and results at work, not only for the technologies and services of concern, but also in terms of bearing legal responsibility. HUAWEI CLOUD employees are made well aware that if ever a security issue arises due to a security violation by an employee, it may have grave consequences for customers and the company as a whole. Therefore, HUAWEI CLOUD always holds employees accountable based on behavior and results, regardless of their intent. HUAWEI CLOUD will determine the nature of an employee's security violation and the level of his or her accountability based on the consequences and take disciplinary actions accordingly. Cases will be handed over to law enforcement if legal violations are involved. Direct and indirect management must also bear responsibility for their negligence, substandard management, and condonation for security violation(s) by their employee(s). In handling security violations, HUAWEI CLOUD also factors in the perpetrator's attitude and cooperation during the investigation and adjusts the punishment severity accordingly before meeting it out.<br>**(3)** HUAWEI CLOUD data centers employ industry standard data center physical security |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | 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. Security guards routinely patrol data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms. |
| Access Controls -10.26 and 10.27 | 10.26 FSPs must identify the location of customer information residing in different systems and ensure that adequate access controls are in place at different levels (i.e. application level, database level, operating system level and network level) to prevent unauthorized access, modification or disclosure by whatever means of customer information to external parties.<br>10.27 FSPs must regularly review the access rights of staff and immediately revoke the access rights of a staff leaving the FSP or changing to a new role or position that does not require access to customer information to prevent the theft of customer information. | Customers should establish an access control mechanism for customer information to prevent unauthorized access to the system, and regularly review the access rights of staff, immediately revoke the access rights of a staff leaving the company and update the rights of transfer staff.<br>Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**.<br>Huawei Cloud's | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** Except for support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists.<br>**(2)** HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | **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. | centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to realize that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different responsibilities in different positions are limited to access the equipment under their role. |
| Physical Security -10.28, 10.29, and 10.32 | 10.28 FSPs must implement adequate physical security controls to ensure customer information stored either in paper or electronic forms are properly protected against theft, loss, misuse or unauthorized access, modification or disclosure by whatever means.<br>10.29 FSPs must restrict access and employ robust intruder deterrents to areas where large amounts of customer information is accessible and stored, for example, the server and filing rooms.<br>10.32 To effectively safeguard customer information throughout its lifecycle, FSPs must | Customers should establish physical security management mechanisms, restrict access to areas where large amounts of customer information is accessible and stored to prevent customer information from being stolen, lost, or unauthorized use. In addition, the customer should also identify the customer information that is no longer needed, and adopt an appropriate way to dispose. | As a cloud service provider:<br>**(1)** HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standard of *TIA-942 Telecommunications Infrastructure Standard for Data Centers*. 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 and appropriate data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | have proper procedures in place to identify customer information that is no longer required from the perspective of operation or requirements of any written law. FSPs shall deploy appropriate methods to securely dispose of such customer information which includes any paper and digital records of the customer information. | | the demands of tomorrow's rapid infrastructure expansion. The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers.<br>**(2)** HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. Security guards strictly review and regularly review the users' access authorizations. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system. Designated personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis so that unauthorized personnel have no access to data centers. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | **(3)** 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 effective data protection possible in order to support the privacy, ownership, and control of our users' data against data breaches and impacts on their business. When customers stop using HUAWEI CLOUD services and need to destroy content data, HUAWEI CLOUD clears the specified data and the copies. 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 so the 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 so that data on the storage medium cannot be restored. |
| Staff, Representatives, Agents and External Vendors' Personn | 10.39 FSPs must ensure that employment contract contains a provision requiring all staff to sign a confidentiality undertaking that clearly specifies the obligation and | Customers should require all staff to sign a confidentiality undertaking that clearly specifies the obligation and requirement of safeguard | As a cloud service provider:<br>**(1)** HUAWEI CLOUD has established, and continued to improve, a complete information security and privacy protection management system in accordance with various regulatory requirements, international and industry standards. The |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| el - 10.39, 10.40, 10.42, 10.43, 10.44, 10.45, 10.49, and 10.50 | requirement of any written law to safeguard customer information as well as the consequences for failure to comply with such obligation and requirement.<br>10.40 Where FSPs engage with external vendors to carry out duties or services within the FSPs' premises (e.g. security guards, cleaners and maintenance officer/ engineer), FSPs must ensure that the external vendors carry out an appropriate level of vetting and monitoring on their personnel to reduce the risk of customer information theft.<br>10.42 FSPs must have in place robust monitoring to ensure that the relevant policies, procedures and controls established by the FSPs are being adhered to by staff.<br>10.43 FSPs must provide relevant training and regularly remind all staff on their obligations to properly handle customer information.<br>10.44 FSPs must include in their program for new staff a specific training to explain the relevant policies and procedures on protecting customer information.<br>10.45 New staff must | customer information. Customers should have in place robust monitoring to ensure that the security policies are being adhered to by staff, and request the external vendors carry out an appropriate level of vetting and monitoring on their personnel. In addition, customers should conduct information security awareness training for employees, and investigate and appropriately handle employees who violate security policies. | management system has detailed policies and procedures in many security fields, such as physical security control, system security, security awareness training and so on. HUAWEI CLOUD continues to implement management system requirements to ensure customer business and data security.<br>**(2)** HUAWEI CLOUD has formulated a comprehensive security awareness training plan, which includes various forms of employee recruitment, on-the-job, transfer, and other such types of security awareness training. This makes employees' behavior complies with all applicable laws, policies, processes and requirements in Huawei's business code of conduct.<br>**(3)** HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the HUAWEI CLOUD according to the situation.<br>**(4)** Huawei has established a rigorous security responsibility system and implemented accountability measures against security violations. On the one hand, Huawei Cloud carries out our responsibilities in accordance with the shared responsibility model and takes full responsibility for any security violation caused by Huawei Cloud in order to minimize user business impact. On the other |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | also be alerted by the FSPs on the possible actions that may be taken for non-compliance with policies and procedures.<br>10.49 FSPs must conduct a thorough and timely investigation upon detecting theft, loss, misuse or unauthorized access, modification or disclosure by whatever means of customer information by staff and take appropriate actions against the staff concerned.<br>10.50 The actions taken pursuant to paragraph 10.49 must send a strong message to all staff and act as deterrent to prevent future recurrence of the customer information breach. | | hand, Huawei Cloud mandates that every employee be responsible for his/her actions and results at work, not only for the technologies and services of concern, but also in terms of bearing legal responsibility. Huawei Cloud employees are made well aware that if ever a security issue arises due to a security violation by an employee, it may have grave consequences for customers and the company as a whole. Therefore, Huawei Cloud always holds employees accountable based on behavior and results, regardless of their intent. Huawei Cloud will determine the nature of an employee's security violation and the level of his or her accountability based on the consequences and take disciplinary actions accordingly. Cases will be handed over to law enforcement if legal violations are involved. Direct and indirect management must also bear responsibility for their negligence, substandard management, and condonation for security violation(s) by their employee(s). In handling security violations, Huawei Cloud also factors in the perpetrator's attitude and cooperation during the investigation and adjusts the punishment severity accordingly before meeting it out. |
| Independent Review -10.53 | FSPs must subject their policies, procedures and control measures for safeguarding customer information to an independent review at least once in every two years. | Customers should regularly subject their policies, procedures and control measures for safeguarding customer information to an independent review. | As a cloud service provider, if an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible person to actively cooperate regarding the audit. 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 has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | protection certifications, and is audited by third party every year. |

# 7.2 Customer Information Breaches

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Customer Information Breaches -11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.12, and 11.13 | 11.1 FSPs must have in place a customer information breach handling and response plan in the event of theft, loss, misuse or unauthorized access, modification or disclosure by whatever means of customer information.<br>11.2 The plan by FSPs under paragraph 11.1 must at a minimum, include escalation procedures and a clear line of responsibility to contain the customer information breach and take remedial actions.<br>11.3 FSPs must ensure that staff understands the escalation procedures and relevant staff are trained to take the appropriate remedial action to a customer information breach effectively to protect affected customers' interests.<br>11.4 FSPs must have in place a mechanism to identify customer information breaches including those which arise from customer complaints and investigate the complaints promptly and properly.<br>11.5 FSPs must take | Customers should establish a customer information breach incident management mechanism, formulate customer information breach handling and response plan, clarify the escalation procedures and personnel responsibilities, establish identify customer information breaches procedures, and take appropriate mitigating actions. In addition, customers should also assess the impact and notify customers in time. | As a cloud service provider:<br>**(1)** HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. 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. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | appropriate mitigating actions to contain a customer information breach immediately.<br>11.6 FSPs must assess the impact arising from the theft, loss, misuse or unauthorized access, modification or disclosure by whatever means of customer information.<br>11.12 In the event the customer information breach affects a large number of customers, FSPs must assess the potential impact and take appropriate actions to avoid or reduce any harm on the affected customers.<br>11.13 The actions referred to in paragraph 11.12 may include the following:<br>(a) making a public announcement to notify the customers promptly to regain customers' confidence;<br>(b) providing contact details for customers to obtain further information or raise any concern with regard to the breach; or<br>(c) providing advice to affected customers on protective measures against potential harm that could be caused by the breach. | | logs for unified analysis of a variety of security devices.<br>**(2)** HUAWEI CLOUD formulates the classification and escalation principles 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.<br>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.<br>**(3)** HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate. The test scenarios are combined with the current common network security threats, in which high-risk scenarios will be tested during simulations. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After their completion, relevant personnel will redact a report and summarize any problems identified during the simulation. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | If the results are indicating issues with the information security incident management and process, related documentation will be accordingly updated.<br>HUAWEI CLOUD regularly reviews and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes. |

# 7.3 Outsourced Service Provider

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Outsourced Service Provider (OSP)-12.2, 12.3, 12.4, 12.6, and 12.7 | 12.2 FSPs must perform adequate and relevant due diligence assessments when selecting an OSP which has access to customer information including for processing, storing, or disposing customer information.<br>12.3 FSPs must be satisfied that the OSP has in place policies, procedures and controls that are comparable to that of the FSPs, to ensure that customer information is | Customers should establish a security management mechanism for outsourcing service providers, perform diligence assessments on the service provider and ensure that the service provider has in place appropriate security policies, procedures and controls. Customers | In order to cooperate with customers to meet regulatory requirements:<br>**(1)** HUAWEI CLOUD will assign a responsible person to actively cooperate regarding the audit and due diligence initiated by customers. HUAWEI CLOUD places great importance to its users' data information assets and regards data protection as the core of Huawei's cloud security policy. HUAWEI CLOUD will continue to follow industry-leading standards for data security lifecycle management using excellent technologies, practices, and processes to support the privacy of users' data in terms of authentication and access control, rights management, data isolation, transmission security, storage security, data deletion, physical destruction, and data backup |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | properly safeguarded at all times.<br>12.4 In ensuring the obligation to safeguard customer information is adequately reflected in the Service Level Agreement (SLA) with an OSP, at a minimum, the SLA must require the OSP to:<br>(a) undertake to safeguard the customer information and prevent any theft, loss, misuse or unauthorized access, modification or disclosure by whatever means;<br>(b) ensure the adequacy and effectiveness of its policies and procedures to protect the FSP's customer information;<br>(c) conduct robust vetting on its personnel who handles customer information;<br>(d) only allow its personnel access to customer information strictly for the purpose of carrying out their functions;<br>(e) ensure that its personnel understands and undertakes to comply with the prohibition on disclosure by whatever means of customer information to any person for any purpose other than | should also sign service level agreement and confidentiality agreement with the service provider to ensure the obligation to safeguard customer information. In addition, customers require service providers to conduct training to its staff, as well as reviews the adequacy and effectiveness of the training plan. | recovery. Inviolable ownership and control are necessary to provide users with the effective data protection. In addition, HUAWEI CLOUD has formulated an emergency response plan, which specifies the organization, procedures, and operating standards of emergency response in detail, and conducts regular tests to ensure continuous operation of cloud services and protect customers' business and data security.<br>**(2)** According to ISO 27001, HUAWEI CLOUD has built a perfect 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. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort.<br>**(3)** HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | that which is specified in the SLA, permitted under the written law or approved by the Bank, as the case may be (including after the end of the contract term);<br>(f) investigate any customer information breach to determine when and how the breach occurred;<br>(g) report any customer information breach to the FSP within an agreed timeframe;<br>(h) destroy in accordance with paragraph 10.32 or return all customer information to the FSP upon the expiry or termination of the SLA;<br>(i) allow the FSP to audit or inspect how customer information is safeguarded.<br>12.6 FSPs must require the OSP to sign a binding non-disclosure undertaking with regard to the handling of customer information.<br>12.7 FSPs must ensure that the OSP conducts training to its staff, at regular intervals, on relevant policies and procedures relating to the proper handling of customer information as well as reviews the | | **(4)** HUAWEI CLOUD will not use customer data for commercial monetization and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the applicable laws and regulations or the binding orders of the government institutions. If a customer initiates a confidentiality requirement, HUAWEI CLOUD will arrange a specialist to actively cooperate. HUAWEI CLOUD will avoid unauthorized information disclosure, the expected actions to be taken in termination or in violation of agreement, and the audit and supervision rights of customers on HUAWEI CLOUD, and the responsibilities and actions of HUAWEI CLOUD will be contained in the signed agreement.<br>**(5)** HUAWEI CLOUD has formulated a comprehensive security awareness training plan, which includes various forms of employee recruitment, on-the-job, transfer, and other such types of security awareness training. This makes employee behavior complies with all applicable laws, policies, processes and requirements in Huawei's business code of conduct. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | adequacy and effectiveness of the training program. | | |

# 8 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Guidelines on Data Management and MIS Framework for Development Financial Institutions

BNM released *Guidelines on Data Management and MIS Framework for Development Financial Institutions* on May 9, 2011. This policy set FIs' customer data management and MIS framework guiding principles from the perspectives of data governance, internal controls and reviews, data architecture and other domains.

When FIs are seeking to comply with the requirements provided in *Guidelines on Data Management and MIS Framework for Development Financial Institutions*, 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 *Guidelines on Data Management and MIS Framework for Development Financial Institutions*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Principle 2 - Data Governance - 4.12 | Where data is managed by third party service providers under outsourcing arrangements, senior management must ensure that effective oversight, review and reporting arrangements are established to ensure that service level agreements regarding standards on data quality, integrity and accessibility are observed at all times. | Please refer to **5.3 Technology Audit** of this document. | Please refer to **5.3 Technology Audit** of this document. |
| Principl | The FI should establish | Please refer to the | Please refer to the |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| e 3 - Data Architecture - 4.14(VI) | appropriate data storage and back-up processes that optimize the functioning of data systems and enable efficient and timely access to data for the purpose of business continuity management. | control domain of **"Data Center Resilience - Data Center Operations"** under **5.1 Technology Operations Management** of this document. | control domain of **"Data Center Resilience - Data Center Operations"** under **5.1 Technology Operations Management** of this document. |
| Principle 5 - Internal Controls and Reviews - 4.20, 4.23, 4.25, and 4.27 | 4.20 FIs must establish adequate preventive and detective controls to ensure that logical and physical access to systems and data is secure and only available to authorized personnel for specific purposes.<br>4.23 Access rights to systems and data should be clearly defined, documented and where appropriate, segregated to prevent critical data or systems from being compromised. Given the sensitivity of the bulk of data handled by FIs, access should generally be given on a "need to know" basis.<br>4.25 Access to critical data or systems by external parties (e.g. system vendors and service providers) must be properly authorized. FIs must ensure that such access by external parties is closely supervised, monitored and appropriately restricted in line with the purpose of the access given. Legal agreements for services contracted should clearly prohibit the unauthorized disclosure of confidential data by the external party and provide for adequate remedies to the FI.<br>4.27 Appropriate safeguards should be put in place to ensure that personal data is not misused or disclosed in a wrongful manner. Personal | Please refer to the control domain of **"Access Control"** under **5.1 Technology Operations Management** and the control domain of **" Control Measures - Information and Communication Technology ICT) Controls"** under **7.1 Control Environment** of this document. | |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | information (of customers, employees or any other parties that the FI may conduct business with) should be handled properly to ensure confidentiality of the information and compliance with relevant legislation. | | |

# 9 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Business Continuity Management

The National Bank of Malaysia released the Business Continuity Management on December 19, 2022. The policy sets out requirements for business continuity management of financial institutions in areas such as the responsibilities of the Board and senior management, notifying banks of disruptions, notifying banks of disruptions, notifying banks of disruptions, and BCM frameworks and methodologies.

When FIs are seeking to comply with the requirements provided in *Business Continuity Management*, 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 on *Business Continuity Management*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| 9.15 | To ensure continued availability of the essential services, a financial institution must have in place contingency arrangements to provide these essential services during a disruption and incorporate these arrangements in the BCP. This includes services which are performed by service providers on behalf of the financial institutions under outsourcing arrangements. | Customer should develop BCP and contingency arrangements based on risk preference and scenarios, including services provided by service providers on behalf of financial institutions according to outsourcing arrangements. | 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. 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. HUAWEI CLOUD security drill team regularly develops policies for different product types |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | (including basic services, operation centers, data centers, and overall organizations) and drills in different scenarios to maintain the effectiveness of the continuity plan. When the organization and environment of HUAWEI CLOUD undergo significant changes, the effectiveness of business continuity is also tested.<br>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 ISO 22301 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 customers is considered as an important criterion for determining key services. |
| 9.25 | To enhance the effectiveness of BCM, a financial institution must incorporate the following requirements and clauses in contractual and outsourcing arrangements with key service providers, suppliers and counterparties:<br>(a) require the key service provider, supplier and counterparty to have in place sound and effective BCP for the outsourced | In the contracts and outsourcing arrangements between customers and key service providers, key service providers are required to make outsourcing arrangements: Develop sound and effective business management plans; Participate | HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | arrangement, including specific MTD and RTO requirements that align with the financial institution's MTD and RTO, and provisions for legal liability if MTD or RTO requirements are not met;<br>(b) require the key service providers to participate in the financial institution's integrated testing, as stipulated in paragraph 9.50(d);<br>(c) allow the internal audit of the financial institution or other independent party appointed by the financial institution to review the BCM of the key service provider, supplier and counterparty; and<br>(d) allow the financial institution to have access to all relevant records and information maintained by the key service provider, supplier and counterparty with respect to the outsourced arrangement. | in the comprehensive test of financial institutions; Allow the internal audit of financial institutions or other independent parties designated by financial institutions to review; Financial institutions are allowed to access all relevant records and data related to outsourcing arrangements. | |
| 9.37 | A financial institution must set up its alternate site and recovery site that can be used if the business premise, infrastructure or systems supporting the CBFs become unavailable in the event of a disruption. | Customers should establish their backup sites and recovery sites, and develop disaster recovery plans to support the continuous operation of CBFs. | **Alternate location for technical recovery:**<br>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, |
| 9.38 | For purposes of paragraph 9.37, examples of an alternate site and a recovery site include in-house arrangements, or available through agreement with service providers, or a combination of both options. | | |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | 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.<br>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.<br>**Disaster recovery test:**<br>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. |
| 9.41 | Where the alternate site or recovery site is managed or owned by a third party, a financial institution must ensure its outsourcing arrangements are in accordance with the policy | Customers should establish an outsourcing management mechanism to continuously monitor and | HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | document on Outsourcing, particularly the following:<br>(a) execution of a service level agreement (SLA) between the financial institution and the third-party provider to ascertain the level and type of services to be provided to the financial institution in order to safeguard the interest of the financial institution;<br>(b) mitigation of concentration risks, where the alternate or recovery site provided, managed or owned by the third party will be utilised by several customers or to customers within the same locality or industry. In this regard, the SLA must specifically identify the conditions under which the alternate or recovery site may be used and specify how customers would be accommodated if simultaneous disruptions affect several customers of the service provider;<br>(c) assessment of the capacity and capability of the service provider for use for a reasonably prolonged period;<br>(d) adequacy of physical and logical access controls provided by the service provider to safeguard the alternate or recovery site; and<br>(e) periodic test, continuous review and monitoring on the level and type of service provided and the risk mitigation measures maintained by the financial institution. | regularly review the outsourcing services.<br>Customers can monitor the use and performance of their own cloud resources through HUAWEI CLOUD monitoring Services **Cloud Eye Service (CES)**. HUAWEI CLOUD can also provide service reports according to SLA and customer needs. If Customers need to conduct inspection and due diligence on HUAWEI CLOUD and its operation, HUAWEI CLOUD will organize a dedicated person to assist.<br>HUAWEI CLOUD's unified **Identity and Access Management (IAM)** provides cloud resource access control for customers. With IAM, the customer administrator can manage user accounts and control the accessible to these user accounts.<br>HUAWEI **CLOUD Trace Service (CTS)**provides operating records | HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.<br>**Monitoring of outsourcing arrangements** : HUAWEI CLOUD can provide service reports according to SLA and customer needs. If Customers need to conduct inspection and due diligence on HUAWEI CLOUD and its operation, HUAWEI CLOUD will organize a dedicated person to assist.<br>**Capacity and performance management:** HUAWEI CLOUD has developed standard capacity management and resource prediction programs to manage HUAWEI CLOUD capacity in a unified manner and improve HUAWEI CLOUD resource availability. Based on the input from all parties, HUAWEI CLOUD predicts the future resource capacity in a rolling manner, formulates appropriate resource expansion solutions, and periodically monitors the capacity usage of HUAWEI CLOUD every day, analyzes and evaluates service capacity bottlenecks and performance bottlenecks. When resources reach the preset threshold, HUAWEI CLOUD releases resource warnings and takes further solutions. This prevents the system performance of tenant cloud services from being affected.<br>Huawei Cloud has |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | of cloud service resources for users to query, and for auditing. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within Huawei's cloud system. | 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.<br>Huawei Cloud provides the **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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | performance of instance resources of each service.<br>**Logical access control:** 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.<br>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 gain unauthorized access through minimal privilege assignment and strict behavioral auditing.<br>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.<br>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. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | 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.<br>**Physical access control:** HUAWEI CLOUD enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each HUAWEI CLOUD data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. Security guards strictly review and regularly audit user access privileges. HUAWEI CLOUD requires that visitors be accompanied by internal personnel throughout the whole process and can only travel in restricted areas.<br>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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | integrated with infrared sensors and physical access control systems. Security guards routinely patrol data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms. |
| 9.50 | A financial institution must periodically conduct an integrated testing on a reasonable wide-scale basis for all the CBFs, including those undertaken by the key service providers, commensurate with its size, nature, complexity and risk profile. In doing so, the financial institution must–<br>(a) use backup IT systems to gauge and assess its application system linkages and network connectivity;<br>(b) calibrate the load or capacity requirements that are required to support minimum service levels to be provided during a disruption;<br>(c) include such calibrations in subsequent rounds of testing; and<br>(d) ensure participation of key service providers to evaluate their adequacy and readiness to respond to the recovery measures, that the financial institution needs to deploy during a disruption. | Customers should establish their own business continuity mechanism, develop BCP and BIA, develop MTD and RPO indicators to ensure their key business continuity, and regularly test BCP. | 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.<br>To meet customer compliance requirements, HUAWEI CLOUD not only provides high-availability infrastructure, redundant data backup, and disaster preparedness in available areas, but has also obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. |
| 9.51 | In designing and carrying out the testing, a financial institution must–<br>(a) develop test plans with predetermined test goals, | Customers should develop BCP and DRP, establish emergency plans, conduct regular | To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | scope and test evaluation criteria, using realistic simulations10 and activity volumes;<br>(b) develop metrics to measure effectiveness of the BCP and DRP and the extent to which various business continuity objectives are met;<br>(c) develop necessary contingency measures in the event of failed testing to avoid business disruptions; and<br>(d) maintain formal testing documentation, including test plan, objectives, scenarios, procedures and results, for future reference and audit. | tests, and retain formal test documents. | system that meets its own business characteristics and has obtained the IS0 22301 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. 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. When the organization and environment of HUAWEI CLOUD undergo significant changes, the effectiveness of business continuity is also tested.<br>HUAWEI CLOUD has developed a comprehensive emergency response plan, which specifies the organization, procedures, and operation specifications for emergency response. The plan also conducts regular tests to ensure continuous running of cloud services and ensure customer service and data security.<br>HUAWEI CLOUD strictly records all related information and handling procedures during emergency handling. All process materials should be archived by dedicated personnel. HUAWEI CLOUD has a professional security incident management system, which records and tracks the |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | progress, handling measures, and implementation of all information security incidents, analyzes the impact of incident handling, and tracks security incidents in an E2E manner to ensure that the entire handling process can be traced back. |

# 10 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of BNM Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMIT) Policy Document (Exposure Draft)

The National Bank of Malaysia released the Cloud Technology Risk Assessment Guide (CTRAG) - Appendix to the Technology Risk Management (RMIT) Policy Document on June 3, 2022. The draft for comments covers cloud governance, cloud architecture, cloud application delivery models, virtualization and containerization management, change management, cloud backup and recovery, exit strategies, encryption key management, access control, cybersecurity actions, distributed denial of service (DDoS), data loss prevention (DLP), security operations Center (SOC), network response and recovery requirements.

When FIs are seeking to comply with the requirements provided in *Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMIT) Policy Document (Exposure Draft)*, 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 on *Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMIT) Policy Document (Exposure Draft)*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

## 10.1 Cloud Governance

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Part A: 3. Due diligence | Due diligence on the prospective cloud service providers should be risk- | The customer shall conduct due diligence on the | **Data Storage and Processing Location:** Huawei Cloud has launched |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | based and conducted to a level of scrutiny that is commensurate with the criticality of the information and technology assets to be hosted on the cloud. It should at minimum:<br>(a) Include all locations where all financial institutions' data will be processed and stored;<br>(b) Include an assessment of the potential impact of the cloud outsourcing arrangement on the financial institution's legal, compliance, operational, information security, data privacy and reputational risks;<br>(c) Address relevant requirements and guidance as stipulated in the Third-Party Service Provider Management section of the RMiT policy document and related sections in Outsourcing policy document (Outsourcing process and management of risks); and<br>(d) Risk assessment should be promptly reviewed or re-performed upon material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislations and geopolitical development. | cloud service provider according to the review level commensurate with the importance of the information and technology assets to be hosted on the cloud, including data storage and processing location, law, compliance, operation, information security, data privacy and reputation risk. | cloud services in multiple countries and regions. Its infrastructure spans multiple availability zones (AZs) and regions and offers impressive availability and fault tolerance.<br>Huawei Cloud services are divided by region. A region is the physical location where a customer's data is stored. Huawei Cloud will never transfer data between regions without the customer's explicit approval. Customers are advised to select the regions closer to their clients in accordance with service requirements and applicable laws and regulations, and ensure that their data is stored in these regions.<br>For regional services, customers can select a region during purchase and change the service deployment location and data retention location on the Huawei Cloud portal, if required.<br>**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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | system.<br>**Compliance**: In regions within our cloud service coverage, Huawei Cloud actively facilitates dialogue with local regulators to better understand their concerns and requirements, share Huawei Cloud's knowledge and experience, and continue to bolster the legal and regulatory compliance posture of Huawei Cloud's technologies, services, and security. Additionally, Huawei Cloud shares its legal and regulatory insights with customers, avoiding violations caused by inadequate information disclosure. While ensuring that tenant contracts accurately specify the security responsibilities of both sides, Huawei Cloud continuously complies with regulatory requirements by obtaining cross-industry, cross-region cloud security certifications. It continues to foster and strengthen customer trust by gaining security certifications that target key industries and regions, striving toward a secure cloud environment built by law-makers, cloud platform administrators, and tenants.<br>**Information Security**:<br>Huawei Cloud focuses on data protection, leverages the company's strong security R&D capabilities, and develops and adopts world-leading technologies, striving toward the creation of a highly reliable and intelligent cloud security system and highly automated cloud |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | security O&M. Additionally, through big data analysis of network security posture, Huawei Cloud identifies, prevents, mitigates, and resolves major risks, threats, and attacks. It employs a robust multi-layered technological framework for cloud security protection, monitoring, analysis, and response to ensure cloud service O&M security, thereby supporting rapid detection, isolation, and recovery when faced with security risks, threats, and attacks. Huawei Cloud's advanced technologies bring tenants convenience, security, and business value.<br>**Business reputation**: As always, HUAWEI CLOUD adheres to "customer-centricity", enabling more and more customers to choose HUAWEI CLOUD. HUAWEI CLOUD has made major breakthroughs in multiple industries in China, such as the Internet, VOD live broadcast, video surveillance, genetics, and automobile manufacturing.<br>**Data privacy**: Huawei Cloud has established a complete privacy protection system. It has established a series of privacy protection policies from the company and process levels to protect the privacy of customers. At the same time, it has established a department and full-time staff dedicated to privacy protection to inspect, reduce and verify the effective implementation of privacy protection measures within Huawei Cloud every |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | year. |
| Part A: 4. Access to authoritative third-party certifications | A financial institution should review their cloud service providers' certifications prior to cloud adoption. At a minimum, a financial institution should:<br>(a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider`s action plans for mitigating any non-compliance; and<br>(b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. This should address requirements and guidance as stipulated in the Cloud Services section of the RMiT policy document and Outsourcing involving Cloud Services section in Outsourcing policy document. | Before adopting cloud technology, customers should review the certification of their cloud service providers. | HUAWEI CLOUD has passed multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR, and is audited by a third party every year.<br>Additionally, Huawei Cloud shares its legal and regulatory insights with customers, avoiding violations caused by inadequate information disclosure. While ensuring that tenant contracts accurately specify the security responsibilities of both sides, Huawei Cloud continuously complies with regulatory requirements by obtaining cross-industry, cross-region cloud security certifications. It continues to foster and strengthen customer trust by gaining security certifications that target key industries and regions, striving toward a secure cloud environment built by law-makers, cloud platform administrators, and tenants. |
| Part A: 5. Contract management (a) | (a) A financial institution should set out clearly and where relevant, measurable, contractually agreed terms and parameters on the information security and operational standards expected of the cloud service provider. Such contract terms and parameters should be aligned with the financial institution's business strategy, information | The customer should formulate clear, measurable and contractually agreed terms and parameters with the expected cloud service provider, and the contract terms should address the risks related to cloud services specified in the cloud services section of | HUAWEI CLOUD provides the HUAWEI CLOUD User Agreement and HUAWEI CLOUD Service Level Agreement, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | security policies and regulatory requirements. The terms of the contract between the financial institution and cloud service provider should address the risks associated with cloud services as stipulated in the Cloud Services section of the RMiT policy document. | the RMiT policy document and Outsourcing involving Cloud Services section in Outsourcing policy document. | customer requirements.<br>Huawei Cloud has obtained many international and industrial security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, CSA STAR, etc. Huawei Cloud establishes information security management system, IT service management system and business continuity management system in accordance with international standards, and implements the requirements of the system in daily operation. At the same time, Huawei Cloud regularly carries out risk assessment, management review and other activities every year to identify problems in the operation of the system, implement rectification and promote the continuous improvement of the management system. |
| Part A: 5. Contract manage ment (b) | (b) The contract terms, obligations, and responsibilities of all contracting parties (this may include sub-contractor(s) if the sub-contractor is material to the provision of critical function(s)) should be explicitly stated in the contract. At a minimum, the contract should address requirements and guidance as stipulated in Third-Party Service Provider Management sections of the RMiT policy document and related sections in the Outsourcing policy document (Outsourcing | The contract agreement signed by the customer and the cloud service provider should specify the contract terms, obligations and responsibilities of all contractors, and address requirements and guidance as stipulated in Third-Party Service Provider Management sections of the RMiT policy document and related sections in | HUAWEI CLOUD provides the HUAWEI CLOUD User Agreement and HUAWEI CLOUD Service Level Agreement, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.<br>Customers' rights and interests in auditing and monitoring HUAWEI CLOUD will be promised in agreements signed with FIs |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | agreement and Protection of data confidentiality). | the Outsourcing policy document (Outsourcing agreement and Protection of data confidentiality). | based on actual situations. |
| Part A: 5. Contract manage ment (d) | (d) Difficulties related to incident response and investigation may arise with cloud services as financial institutions may no longer have full access to the computing components managed by the cloud service providers as compared to an on-premises solution. At a minimum, a financial institution should assess the potential impact and formalise arrangements with cloud service providers to comply with local laws and regulatory requirements for incident investigation and law enforcement purposes. This would include adhering to data retention requirements and data access procedural arrangements to ensure the confidentiality and privacy of the customers are protected. | The customer shall require the cloud service provider to comply with local laws and regulatory requirements through the agreement and arrangement with the cloud service provider to conduct incident investigation and law enforcement. | HUAWEI CLOUD provides the HUAWEI CLOUD User Agreement and HUAWEI CLOUD Service Level Agreement, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. |
| Part A: 5. Contract manage ment (e) | (e) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth-party cloud service providers (sub-contractors), which could change rapidly. For example, customer data were leaked due to exposure made by fourth | The customer shall ensure that Service Level Agreement (SLA) negotiations and contractual terms cover the performance matrix, availability, and reliability of services to ensure all parties agree | In line with customer regulation for technology outsourcing, the online HUAWEI CLOUD Customer Agreement divides the security responsibilities of cloud service customers and Huawei, while the HUAWEI CLOUD Service Level Agreement defines the level of services provided by HUAWEI CLOUD. HUAWEI CLOUD has also |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | party. To mitigate fourth-party risks, financial institutions should:<br>i) understand the scope of customer information shared across the supply chain and ensure that relevant information security controls can be legally enforced [by the financial institution]; and<br>ii) ensure Service Level Agreement (SLA) negotiations and contractual terms cover the performance matrix, availability, and reliability of services to ensure all parties agree and are formally aligned on the requirements and standard of services provided. | and are formally aligned on the requirements and standard of services provided. | developed an offline contract template, which stipulates that if HUAWEI CLOUD should hire subcontractors, HUAWEI CLOUD shall notify customers and be responsible for the subcontracting services according to customer requirements.<br>HUAWEI CLOUD has developed its own mechanism for supplier management as suppliers have raised their security requirements for their own products and internal management. In addition, HUAWEI CLOUD will also conduct regular audits of suppliers as at-risk suppliers will be audited on-site. Moreover, network security agreements are signed with vendors involved in network security, and the quality of service is continuously monitored as vendor performance is evaluated during the service process, and vendors with consistently poor security performance will be downgraded.<br>The HUAWEI CLOUD Service Level Agreement stipulates the service level of Huawei Cloud products/services, including the commitment to service availability and service compensation for failure to meet the commitment. |
| Part A: 6. Oversight over cloud service providers | A financial institution should ensure effective oversight over cloud service providers and the cloud service providers' sub-contractor(s). This includes, at a minimum, | Customers should effectively supervise cloud service providers and their subcontractors. | HUAWEI CLOUD can provide service reports according to SLA and customer needs. If Customers need to conduct inspection and due diligence on HUAWEI CLOUD and |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | the following:<br>(a) Establish and define a continuous monitoring mechanism with alignment to the enterprise vendor management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis;<br>(b) Identify, assign and document the key responsibilities within the financial institution for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined; and<br>(c) Perform periodic assessments of the cloud service provider`s control environment, including business continuity management, to assess the potential impact on the financial institution's business resilience. This should address the requirements and guidance of Outsourcing involving Cloud Services section in Outsourcing policy document. | Customers can monitor the usage and performance of their cloud resources through the **HUAWEI CLOUD Eye Service (CES).** | its operation, HUAWEI CLOUD will organize a dedicated person to assist.<br>Customers' 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 customers and assign dedicated personnel to actively cooperate with Customers and financial transaction entities to supervise and supervise the audit and supervision of HUAWEI CLOUD.<br>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, and regularly test the backup and recovery procedures.<br>If Huawei Cloud is required to assist in implementing the customer's disaster recovery |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | plan, Huawei Cloud will actively cooperate. Huawei Cloud will notify customers in advance if they need to participate in the disaster testing process of Huawei Cloud.<br>Simultaneously, HUAWEI CLOUD has developed its own business continuity plan, in addition to providing features such as improved infrastructure availability, redundant data backup, and disaster preparedness in available areas. The program focuses on major disasters such as earthquakes or public health crises to keep cloud services running and secure the customer business and data. |

# 10.2 Cloud Design and Control

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Part B: 1. Cloud architecture (b) | (b) A financial institution is encouraged to adopt zero-trust principles2 to provide enhanced access control via micro-segmentation of application and infrastructure with “deny-by-default”, “least privilege” access rights or on a ‘need-to-have’ basis. | Huawei Cloud provides **Identity and Access Management (IAM)** for customers to manage their accounts that use 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 | 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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | 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. | 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.<br>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 gain unauthorized access through minimal privilege assignment and strict behavioral auditing.<br>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.<br>Privileged Account Management System binds functional or technical accounts of daily or emergency operations to operation and maintenance teams or individuals. Strong |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | log auditing is supported on the bastion host to ensure that the operation and maintenance personnel's operations on the target host can be located to individuals. Grant privileged or emergency accounts to employees only when necessary for their duties. All applications for privileged or emergency accounts are subject to multiple levels of review and approval. |
| Part B: 1. Cloud architecture (d) | (d) A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. This includes the use of a network segregated from production networks for cloud migration and on-going administration of the management plane. | Customers should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms.<br>When customers provide web services over the Internet, they can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. This section describes how to apply for and configure certificates for websites to implement trusted identity authentication and secure transmission based on encryption protocols. In hybrid cloud | Huawei Cloud implements data isolation on the cloud through the Virtual Private Cloud (VPC), and the VPC uses network isolation technology to isolate tenants at Layer 3. Tenants can control the construction and configuration of their own virtual networks. A tenant's VPC can be connected to a traditional data center on the tenant's intranet through a VPN or Direct Connect. This allows the tenant's applications and data residing on its intranet to be seamlessly migrated to the tenant's VPC. Furthermore, the ACL and security group functions of the VPC can be used to configure security and access rules according to the tenant's specific requirements for finer-grained network isolation.<br>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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | deployment and global deployment scenarios of FIs, services such as **Virtual Private Network (VPN)**, **Direct Connect (DC)**, and **Cloud Connect (CC)** provided by HUAWEI CLOUD can be used to implement service interconnection and data transmission security between different regions.<br>FIs can use **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD to migrate data from local data centers to HUAWEI CLOUD. OMS and SMS support mainstream public cloud vendors in China and abroad. SMS also supports VM migration on the private cloud platform and x86 physical servers (covering about 40 mainstream operating systems). | 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. |
| Part B: 2. Cloud applica | (b) Cloud application delivery models may evolve to support faster time-to-market in response | Customers should establish their own cloud application delivery process to | Due to the changed business model of Huawei Cloud services, Huawei Cloud has established a new |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| tion deliver y models (b) | to consumer demand. Currently, DevOps and Continuous Integration / Continuous Development (CI/CD)7 are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A financial institution should ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure. | ensure proper service configuration. | organizational structure and management system and adopted the DevOps process, which is more suitable for cloud service development, deployment, and operations. DevOps is different from traditional ICT R&D processes. Huawei Cloud has adopted the new and rapidly iterative DevOps process, which supports continuous integration, delivery, and deployment. In addition, Huawei Cloud has incorporated the R&D and O&M security requirements of high reliability and stability into the DevOps process to form the DevSecOps process.<br>Huawei Cloud strictly complies with Huawei's secure coding standards. Before taking up positions, Huawei Cloud service development and testing personnel are all required to learn the corresponding standards and pass examinations. In addition, Huawei Cloud introduces static code scanning tools for daily checks, with the resulting data fed into the cloud service CI/CD tool chain to control code quality via thresholds and assess the quality of cloud services and products. All alarms generated during static code scanning must be cleared before any cloud service is released, thereby preventing code-related security issues before service rollout. |
| Part B: 3. Virtuali zation | The guidance provided in this paragraph is relevant for PaaS and IaaS cloud service models. | Customers should consider establishing standardized | HUAWEI CLOUD provides an image service to support **Elastic Cloud Service (ECS)**. Customers can |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| and containerization management | (a) A financial institution should ensure virtualization services are configured in line with the prevailing guidance from the cloud service provider and industry best practices, commensurate with the evolution of cloud computing technologies.<br>(b) A financial institution should ensure virtual machine and container images are configured, hardened, and monitored appropriately. This includes the following:<br>i) use latest images and keep images up to date;<br>ii) store and use images from trusted repositories or registries;<br>iii) scan images for vulnerabilities, remediate any vulnerabilities prior running in production;<br>iv) enforce “least privilege” access;<br>v) harden images based on industry best practices; and<br>vi) stored images are subjected to security monitoring from unauthorised access and changes. | release process to ensure virtual machine and container images are configured, hardened, and monitored appropriately..<br>HUAWEI CLOUD **Image Management Service (IMS)** provides simple and convenient self-service management functions for images, enabling tenants to manage their images through the IMS console or API. Huawei Cloud periodically provides users with public images that have security patches installed, as well as relevant security hardening and patch information as a reference for users during O&M activities, such as deployment, testing, and troubleshooting. Users can directly use a public image, create a private image through an existing elastic cloud server or an external image file, or participate in the development and maintenance of a shared image. They can apply for | choose standard or privatized images provided by the HUAWEI CLOUD official website. Version and release management can be easily carried out through the console.<br>Huawei Cloud periodically provides users with public images that have security patches installed, as well as relevant security hardening and patch information as a reference for users during O&M activities, such as deployment, testing, and troubleshooting.<br>IMS uses IAM for authentication, IMS checks tenants' permissions of all operations and allows only operations with<br>required permissions. It also keeps audit logs of all key operations. In addition, a comprehensive change management procedure prevents HUAWEI CLOUD internal O&M personnel from changing system configuration parameters without authorization.<br>In addition, HUAWEI CLOUD guarantees the security of customer information in multi-tenant scenarios using network isolation, data isolation, external threat defense, identity authentication, access control, and more. For more details, please refer to the HUAWEI CLOUD Security White Paper.<br>Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | an elastic cloud server by using any of these images.<br>UAWEI CLOUD **SoftWare Repository for Container (SWR)** provides easy-to-use, secure, and reliable management of container images throughout their lifecycle, facilitating the deployment of containerized services. SWR allows tenants to securely host and efficiently distribute images on the cloud without building or maintaining image repositories. In addition, it can be used together with CCE and Cloud Container Instance (CCI) for smooth migration of containers to the cloud.<br>HUAWEI **CLOUD Eye Service (CES)** provides users with a threedimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings | 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.<br>For Image security scanning, Tenants can scan uploaded images with one click to identify vulnerabilities in the images, and obtain remediation suggestions. This helps users obtain secure images.<br>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.<br>Huawei Cloud's professional security team performs security hardening on public images and patches any |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | regarding cloud resources and take corresponding measures. | 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. |
| Part B: 5. Cloud backup and recover (a) | (a) As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following:<br>i) define and formalise backup and recovery strategy at the planning stage of cloud adoption;<br>ii) conduct periodic reviews of the cloud service providers' restoration and recovery capabilities;<br>iii) for critical system hosted on cloud, conduct testing of recovery strategy prior deployment of the system. | Customers should establish cloud backup and recovery procedures to ensure that data is not lost in the event of a disaster.<br>HUAWEI CLOUD's **Cloud Backup and Recovery (CBR)** provides backup protection services for EVS disks, elastic cloud servers, and bare metal servers (EVS disks will be referred to as disks, and elastic cloud servers and bare metal servers will be referred to as servers in subsequent text). It also supports snapshot-based backup services, | 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.<br>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 |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | and can use backup data to restore data on servers and disks. In addition, CBR can synchronize backup data in the offline backup software BCManager, manage backup data on the cloud, and restore backup data to other servers on the cloud. CBR supports integrity check of backup data.<br>HUAWEI CLOUD provides **Storage Disaster Recovery Service (SDRS)** for FIs to quickly recover services at DR sites and shorten service interruption time. This service protects service applications, replicates ECS data and configuration information to the DR site, and allows the server where the service applications reside to start and run properly from another location when the server is down, improving service continuity. | 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.<br>HUAWEI CLOUD also deploys a global load-balanced management center, where the customers' applications enable N+1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. |
| Part B: 5. Cloud backup | (c) A financial institution should ensure sufficient backup and recovery of virtual machine and | Customers should ensure sufficient backup and recovery of virtual | In terms of backup and disaster recovery, customers can choose the corresponding backup and |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| and recover (c) | container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following:<br>i) ensure the capability to restore a virtual machine and container at point-in-time9 as per the business recovery objectives;<br>ii) make virtual machine and container images available in a way that would allow the financial Institutions to replicate those images at alternate and recovery site10 ; and<br>iii) allow virtual machine and container images to be downloaded and ported to new cloud service providers. | machine and container including backup configuration settings.<br>HUAWEI CLOUD's **Cloud Backup and Recovery (CBR)** provides backup protection services for EVS disks, elastic cloud servers, and bare metal servers (EVS disks will be referred to as disks, and elastic cloud servers and bare metal servers will be referred to as servers in subsequent text). It also supports snapshot-based backup services, and can use backup data to restore data on servers and disks. In addition, CBR can synchronize backup data in the offline backup software BCManager, manage backup data on the cloud, and restore backup data to other servers on the cloud.<br>The **Cloud Data Migration (CDM)** service enables data migration among multiple types of data sources, such as database s, data | disaster recovery services to realize the backup and disaster recovery protection required by their business at the hard disk level, server level and virtual machine level.<br>HUAWEI CLOUD provides multigranularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also use the Backup and Archive Solution, backup and archiving software, and HUAWEI CLOUD infrastructure to back up on-premises data to HUAWEI CLOUD.<br>With the DEW service, customers can encrypt backup data easily and quickly, thereby ensuring data security.<br>In addition, to minimize service interruption caused by hardware failures, natural disasters, or other disastrous events, HUAWEI CLOUD has prepared DR plans for all data centers:<br>• User data can be replicated and stored on multiple nodes in a data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | warehouses and files, and supports data migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on premises data centers.<br>Customers can use **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD to migrate data from local data centers to HUAWEI CLOUD. OMS and SMS support mainstream public cloud vendors in China and abroad. SMS also supports VM migration on the private cloud platform and x86 physical servers (covering about 40 mainstream operating systems). | recovery.<br>• 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.<br>HUAWEI CLOUD provides cloud migration services for customers. Based on the information provided by the FIs, HUAWEI CLOUD will work with the customers to negotiate and confirm the specific business objectives and scope, design a migration solution for the customers through requirement analysis, develop a migration plan, and perform migration drills. |
| Part B: 5. Cloud backup and recover (d) | (d) A financial institution should assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. To ensure | Customers should ensure the high availability and redundancy of cloud services, and ensure that production data centers have redundancy capabilities in | 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.<br>Huawei Cloud implements a disaster recovery (DR) and |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | service availability, financial institution should consider a risk-based approach and progressively adopt one or more of the redundancy approaches, including diversifying away from a single CSP. Amongst the viable options are:<br>i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones;<br>ii) achieve geographical redundancy by having data centres in different geographical regions;<br>iii) adopt hybrid cloud (combination of on-premises and public cloud setup);<br>iv) establish back-up cloud service providers and identify appropriate arrangement for porting of data and application to ensure timely service resumption; and<br>v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks. | different availability areas. | 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.<br>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.<br>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). |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| Part B: 6. Interoperability & Portability | Interoperability standards for cloud services continue to evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems and alternate cloud service providers, financial institutions are encouraged to:<br>(a) ensure technical requirements for interoperability and portability are included in the contractual agreement with the cloud service provider to avoid vendor lock-in;<br>(b) maintain a list of cloud service providers and tools that are needed to facilitate a smooth transition;<br>(c) ensure usage of standardized network and communication protocols for ease of interoperability and portability with on-premise IT systems or alternate cloud platforms;<br>(d) ensure the use of common electronic data formats, where applicable, to ease the movement of data between cloud service providers or to on-premises IT system; and<br>(e) extend patch and EOL management to ensure technology solutions employed remain effective and protected against system vulnerabilities. | Customers should ensure that the technical requirements for interoperability and portability are included in the contract agreement with the cloud service provider.<br>The **Cloud Data Migration (CDM)** service enables data migration among multiple types of data sources, such as database s, data warehouses and files, and supports data migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on premises data centers.<br>Customers can use **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD to migrate data from local data centers to HUAWEI CLOUD. OMS and SMS support mainstream public cloud vendors in China and abroad. SMS also supports | HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.<br>HUAWEI CLOUD provides cloud migration services for FIs. Based on the information provided by the FIs, HUAWEI CLOUD will work with the FIs to negotiate and confirm the specific business objectives and scope, design a migration solution for the FIs through requirement analysis, develop a migration plan, and perform migration drills. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | VM migration on the private cloud platform and x86 physical servers (covering about 40 mainstream operating systems). | |
| Part B: 7. Exit strategy (b) | (b) A financial institution's exit strategy should be supported by an exit plan that establishes the operational arrangements to facilitate an orderly exit from a cloud service provider, which include the following:<br>i) conduct impact assessment to determine potential costs, resources and timing implications of transferring cloud services to an alternative cloud services provider or back to in-house arrangement at the financial institution;<br>ii) identify appropriate methods to port data and applications to an alternative arrangement;<br>iii) obtain written confirmation from the cloud service provider or via an independent external service provider's attestation that all sensitive data has been completely removed and destroyed from the cloud service provider's facilities upon completion of the exit process; and<br>iv) conduct testing to validate the effectiveness of the exit plan, to obtain a reasonable degree of assurance of its effectiveness. | Customers should develop an exit plan to ensure the orderly exit from the cloud service provider, including cloud service migration and the complete deletion and destruction of sensitive data from the cloud service provider's facilities after the exit process. | Data destruction refers to destroying data physically or digitally. When a customer proactively deletes data stored on the cloud or the data needs to be deleted<br>because a service has expired, Huawei Cloud will delete the data in compliance<br>with data destruction standards and an agreement signed by the customer.<br>When customer data is destroyed on Huawei Cloud, the data is deleted, along with all its copies. After a user confirms data deletion, Huawei Cloud first deletes the indexing between the user and the data. Then, Huawei Cloud zeroes out the storage resources involved, such as memory and block storage space. This ensures that deleted data and related information cannot be restored or recovered if those storage resources are later reallocated to other users.<br>Huawei Cloud also follows comprehensive storage media disposal procedures based on industry standards to ensure data security at the end of the data center media lifecycle. In compliance with the NIST Special Publication 800-88 guideline, data on the storage media that needs to be reused is overwritten by random numbers, or deleted |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | after encryption. Storage media that does not need to be reused is degaussed or physically destroyed. |
| Part B: 8. Cryptographic key management (a) | (a) A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | Customers should implement appropriate and relevant encryption technologies to protect the confidentiality and integrity of sensitive data on the cloud.<br>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. | Huawei Cloud uses customer master key online redundancy storage, multiple physical offline backups of root keys, and periodic backups to ensure key persistence.<br>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.<br>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.<br>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 |
| Part B: 8. Cryptographic key management (c) | (c) For critical systems hosted on the cloud, financial institutions should retain ownership and control of the encryption key (themselves or with an independent key custodian), independent from the cloud service provider, to minimize the risk of unauthorised access to the data hosted on the cloud. As example, this could be achieved by | Customers should implement a centralized key management system, formulate a unified key management and encryption policy, retain the ownership and control of the encryption key, and reduce the risk of unauthorized | |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | deploying the hardware security module (HSM) on-premises or by utilising HSM-as-a-service from a different cloud service provider. | access to the cloud hosted data.<br>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. DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. DEW allows customers to import their own keys as CMKs for unified management, facilitating seamless integration and interconnection with customers' existing services. | and restoration, and destruction.<br>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 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.<br>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 |
| Part B: 8. Cryptographic key management (d) | (d) Multiple encryption key management systems may add complexity and introduce new challenges of comprehensively maintaining and managing all the cryptographic keys as the usage would increase as cloud adoption increases. A financial institution should consider implementing a centralised key management system to unify key management and encryption policies for efficient scale operation. | | |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | (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. |
| Part B: 9. Access Controls (a) | (a) The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which include the following:<br>i) review the financial institution's patch and EOL management framework to effectively secure the management plan;<br>ii) allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management console;<br>iii) implement "least privilege" and strong multi-factor authentication (MFA) e.g., strong password, soft token, privileged access management tool and | Huawei Cloud provides **Identity and Access Management (IAM)** for customers to manage their accounts that use 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.<br>**Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. It records activities | 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 accounts are used to log in to VPNs and bastion hosts to implement in-depth audit of user logins.<br>In addition to managing the identity and permissions of remote access personnel through Identity and Access Management (IAM), HUAWEI CLOUD also provides encrypted transmission methods for customers to choose from, such as VPN and HTTPS. Additionally, HUAWEI CLOUD only has remote access to its internal systems through the HUAWEI CLOUD unified management access gateway and SVN authority. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | maker-checker functions;<br>iv) employ granular entitlement allocation for privileged users;<br>v) conduct continuous monitoring of the activities performed by privileged users;<br>vi) adopt robust prevention mechanism against phishing and password guessing attacks, credential stuffing and brute-force attacks. e.g., web application firewall (WAF), anti-phishing tools; and<br>vii) ensure secure communication protocols are in place for accessing the management plane. e.g., secure end-to-end communication channels, whitelisting of IP addresses and etc. | in the cloud environment, including VM configurations and log changes, facilitating query and tracing. Combining with Cloud Eye, Customers can monitor user login logs in real time. When malicious logins occur, an alarm is generated and requests from the IP address are rejected.<br>**Cloud Bastion Host (CBH)** is a unified security management and control platform of HUAWEI CLOUD. It helps FIs implement centralized account, authorization, authentication, and audit management. CBH provides cloud computing security management and control systems and components. It integrates functions such as SSO, unified asset management, multi-terminal access protocols, file transfer, and session collaboration.<br>Customers can deploy **Web Application Firewall (WAF)** | Moreover, strong log auditing is supported on the access gateway to ensure that the operation and maintenance personnel can locate their actions on the target host.<br>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 gain unauthorized access through minimal privilege assignment and strict behavioral auditing.<br>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.<br>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 Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | to detect and protect website service traffic from multiple dimensions. | applications for privileged or emergency accounts are subject to multiple levels of review and approval. Huawei Cloud will log in to the tenant console or resource instance only after obtaining the customer's authorization.<br>HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the public-facing network perimeter, trust boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities. In addition, firewall devices are configured to restrict access to Huawei’s production networks. The configurations of firewall policies are configured on machines. A monthly review is performed |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | to ensure firewall rules are configured based on standards. Any changes of firewall rules due to deviations are tracked and remediated. HUAWEI CLOUD restricts the access to high-risk ports and use of high-risk protocols by configuring the firewall policies. |
| Part B: 10. Cybersecurity Operations (b) | (b) The interconnected cloud service supply chain could become a source of cyber risk. A financial institution should ensure integrated monitoring and full visibility of cloud services are established. This should include the following:<br>i) continuous monitoring of system communications between the cloud service provider, on-premise IT systems and other third-party service providers to ensure the security perimeter is not breached; and<br>ii) ensuring that third-party service providers, including those providing ancillary functions, have adequate capabilities to monitor, detect and respond to anomalous activities, with timely communication to the financial institution of relevant cyber incidents. | HUAWEI **CLOUD Eye Service (CES)** provides users with a multidimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures.<br>At the same time, HUAWEI CLOUD can also provide an **Advanced Anti-DDoS Service (AAD)**, **Web Application Firewall(WAF)**, **Database Security Service (DBSS)**, and **Cloud Trace Service (CTS)** to help users accurately and effectively implement comprehensive protection against | 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.<br>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 Cloud security status in real |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | traffic-based attacks and application-level and data-level attacks, as well as reviewing and auditing incidents. | 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.<br>**Incident Detection and Response:** HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices. Incidents will be ranked based on the extent to which security incidents affect the customer's business, and will initiate a customer notification process to notify customers of the incident. After the event is resolved, an event report will be provided to the customer.<br>**Event Disclosure and** |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | **Regulatory Escalation:** To assist customers in meeting the requirements of reporting major risks to stakeholders, HUAWEI CLOUD has set up a 7 x 24 professional security incident response team and expert resource pool to promptly disclose related incidents and notify customers in accordance with laws and regulations, and implement emergency plans and recovery processes to minimize the impact on services. In addition, HUAWEI CLOUD has established a data breach handling mechanism. If necessary, HUAWEI CLOUD will report the incident according to applicable laws and regulations. If the customer needs to monitor and report data, HUAWEI CLOUD will provide related materials with the customer. |
| Part B: 10. Cybersecurity Operations (c) | (c) A financial institution should understand the segregation of responsibility in security management, which varies across the cloud service models. A financial institution should manage the sources of vulnerabilities appropriately including:<br>i) managing vulnerability assessment and penetration testing (VAPT) for cloud services;<br>ii) proactively seek assurance of their cloud service providers to conduct periodic VAPT on the cloud infrastructure to ensure tenant isolation and overall security posture | Customers should establish formal asset management procedures, classify their assets, and define asset owners to quickly identify and fix vulnerabilities in assets.<br>Customers can scan for external vulnerabilities and operating system vulnerabilities. They can detect asset content compliance, scan the configuration to compare it against the | HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and exposure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools (regardless of whether they are found in Huawei or third-party technologies) are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation, |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | remains healthy;<br>iii) understand the cloud service provider's VAPT policy on cloud infrastructure given the varying degree of financial institution's access to the cloud environment, and establish VAPT arrangement upfront;<br>iv) tailor the financial institution`s standard operating procedures for VAPT to the scope of cloud configuration under the financial institution's responsibility. This includes conducting VAPT prior to deployment of cloud services;<br>v) establish appropriate tools to conduct VAPT on cloud services under the financial institution's responsibility, commensurate with the complexity of the cloud environment;<br>vi) the scope of penetration testing should place emphasis on the API calls to the management plane and credentials of privileged users (e.g., cloud administrators), which form the key elements of cyber-attack surface; and<br>vii) the financial institution which adopts high velocity methods e.g., Continuous Integration/Continuous Development (CI/CD), should integrate code review, security testing and vulnerability assessment into the system development life cycle (SDLC) process to | baseline, detect weak passwords, and perform other such functions through HUAWEI CLOUD **Vulnerability Scan Service (VSS)**. It can automatically discover the security risks of websites or servers exposed in the network, and help users to secure their business on the cloud from multiple dimensions. | and its impact to our customers' services. To protect end users and tenants, HUAWEI CLOUD upholds the principle of responsible disclosure. It ensures no undue risks for potential exploitation and attacks will result from the disclosure of any vulnerability, HUAWEI CLOUD continues to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and tenants vulnerability mitigation solutions, standing shoulder to shoulder with our customers to tackle security challenges caused by vulnerabilities.<br>To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal and third party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services. Together with partners, HUAWEI CLOUD has launched host intrusion detection, web application firewall, host vulnerability scanning, web page anti-tampering, and penetration test services, which enhance the security detection, correlation, and protection capabilities of HUAWEI CLOUD.<br>Huawei Cloud Product Security Incident Response Team (CSIRT) has established a mature vulnerability response |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | minimise application vulnerabilities. | | mechanism. For the self-operated cloud, CSIRT continuously optimizes the security vulnerability management process and technical means to ensure rapid remediation of vulnerabilities found in in-house and third-party software used by Huawei Cloud IaaS, PaaS, and SaaS services as well as O&M tools, reducing the risks to tenant services. CSIRT and Huawei Cloud's security O&M team have established a comprehensive mechanism for vulnerability awareness, handling, and disclosure. Huawei Cloud manages vulnerabilities based on its vulnerability management system. It ensures that the vulnerabilities found in the in-house and third-party software are addressed and remediated within the SLA-specified period, thereby preventing vulnerability exploitation from potentially affecting tenant services.<br>Given that a public cloud usually needs to process huge amounts of traffic while also exposed to a wide variety of attacks, 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 detection of ongoing attacks and forecast potential threats. |
| Part B: 13. Security Operati | (b) The responsibilities of cloud service providers with respect to SOC operations should be formalised in the | Customers should specify the responsibilities of the cloud service provider in terms | HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| ons Centre (SOC) (b) | contractual agreement between the financial institution and the cloud service provider, including retention period required for relevant logs needed for forensic purposes and the right of the financial institution to access the logs, to meet the RMiT requirements on access control and security of digital services. | of safe operation in the contract agreement with the cloud service provider, including the retention period required for the relevant logs used for forensics, and the right of financial institutions to access the logs. | specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.<br>HUAWEI CLOUD manages management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems to ensure that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has established a forensic investigation management mechanism and standard evidence collection process based on laws and regulations to support forensic investigation of security incidents. |
| Part B: 14. Cyber respons e and recover (b) | (b) A financial institution should extend its Cyber Incident Response Plan (CIRP) to include adverse scenarios that may affect cloud services and establish clear roles and responsibilities between the financial institution and cloud service providers for incident response and remediation. The incident escalation process and turnaround time should be established with cloud service providers and periodically reviewed, to the extent possible, to achieve an effective incident response. | Customers should establish an incident response plan including adverse scenarios that may affect cloud services, and establish clear roles and responsibilities with cloud service providers to respond for incident response and remediation. | 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 tests information security incident management procedures and processes every year based on internal management requirements. All security incident response personnel, including backup personnel, must participate in the tests. |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | 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. |
| Part B: 14. Cyber respons e and recover (f) | (f) For critical systems hosted on the cloud, a financial institution should establish arrangements with their cloud service providers to conduct annual cyber drills to test the effectiveness of the financial institution's CIRP. | Customers should establish arrangements with cloud service providers to conduct annual cyber drills. | Customers should establish a cybersecurity monitoring mechanism and take effective monitoring measures, including deployment of network monitoring, penetration testing and internal and external audit. In addition, customers should test the effectiveness of their cybersecurity framework at least on an annual basis, taking-into-account security vulnerability assessment, scenario simulation exercise, penetration test, etc. Huawei will cooperate with |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | customers to meet regulatory requirements from the following perspectives:<br>(1) Given that a public cloud usually needs to process huge amounts of traffic while also exposed to a wide variety of attacks, 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 detection of ongoing attacks and forecast potential threats.<br>(2) HUAWEI CLOUD regularly conducts internal practical cybersecurity field exercises (red team and blue team exercises,) and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services.<br>(3) The Huawei Cloud Product Security Incident Response Team (CSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service model, the program ensures rapid patching of vulnerabilities found on in-house-developed and third-party technologies for HUAWEI CLOUD infrastructures, platforms, applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and |

| No. | Control Principle | Customers Considering | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | technical means. In addition, Huawei CSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and make vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless of whether they are found in Huawei's or third-party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to customers. |

# 11 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of SC Guidelines on Management of Cyber Risk

SC released *Guidelines on Management of Cyber Risk* on October 31, 2016. This policy set FIs' cyber risk management requirements from the perspectives of prevention, detection, recovery and other domains.

When FIs are seeking to comply with the requirements provided in *Guidelines on Management of Cyber Risk*, 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 *Guidelines on Management of Cyber Risk*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| 4.5-4.10 | Cyber Risk - Prevention | 4.5 The FI must conduct regular assessments as part of the FI's compliance program to identify potential vulnerabilities and cyber threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks.<br>4.6 The assessment of the vulnerabilities of FI's operating environment must be | Customers should regularly identify and assess potential vulnerabilities and network threats, and formulate preventive measures to minimize the cyber risk, including deploying of anti-virus software, building firewalls, conducting security tests at software development stage, and conducting penetration testing of systems and networks. In addition, customers should conduct appropriate security awareness training for all employees on a regular basis, and regularly review the adequacy and effectiveness of its training plan. As a cloud service provider:<br>**(1)** The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service model, the program ensures rapid patching of vulnerabilities found on in- |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | comprehensive, including making an assessment of potential vulnerabilities relating to the personnel, parties with whom a FI deals with, systems and technologies adopted, business processes and outsourcing arrangements.<br>4.7 The FI must develop and implement preventive measures to minimize the FI's exposure to cyber risk.<br>4.8 Preventive measures referred to in Paragraph 4.7 above may include the following:<br>(a) Deployment of anti-virus software and malware program to detect and isolate malicious code;<br>(b) Layering systems and systems components;<br>(c) Build firewalls to reduce weak points through which attacker can gain access to an entity's network;<br>(d) Rigorous testing at software development stage to limit the number of vulnerabilities;<br>(e) Penetration testing of existing systems and networks; and<br>(f) Use of authority matrix to limit privileged internal or external access rights to systems and data. | house-developed and third party technologies for HUAWEI CLOUD infrastructures, platforms, applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and technical means. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers.<br>**(2)** To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services.<br>**(3)** HUAWEI CLOUD is built upon an appropriate, multi-layered full stack security framework with comprehensive perimeter defense. For example, layers of firewalls isolate networks by security zone, anti-DDoS quickly detects and protects against DDoS attacks, WAF detects and fends off web attacks close to real time, and IDS/IPS detects and blocks network attacks from the Internet in the real time while also monitoring for behavioral anomalies on the host. Given that a public cloud usually needs to process huge amounts of traffic while also exposed to a wide variety of attacks, Huawei Cloud employs its situation awareness analysis system, which correlates security alerts and logs from myriad security appliances, and performs |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | 4.9 The FI must ensure that the board, management, employees and agents undergo appropriate training on a regular basis to enhance their awareness and preparedness to deal with a wide range of cyber risks, incidents and scenarios.<br>4.10 The FI must evaluate improvement in the level of awareness and preparedness to deal with cyber risk to ensure the effectiveness of training programs implemented. | centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats.<br>**(4)** Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, 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 takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services so that the released cloud services can meet the security requirements. Testing is conducted in a test environment, isolated from the production environment, and avoids the use of production data for testing. If production data is used for testing, it must be desensitized, and data cleaning is required after use.<br>**(5)** Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM).** IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists.<br>**(6)** HUAWEI CLOUD has formulated a comprehensive security awareness training plan, which includes various forms of employee recruitment, on-the-job, transfer, and other such types of security awareness training. This makes |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | employee behavior complies with all applicable laws, policies, processes and requirements in Huawei's business code of conduct. |
| 4.11-4.15 | Cyber Risk - Detection | 4.11 In addition to implementing preventive measures, the FI must continuously monitor for any cyber incidents and breaches within its systems and network.<br>4.12 The FI must ensure timely detection of and response to cyber breaches within a clearly defined escalation and decision-making processes to ensure that any adverse effect of a cyber-incident is properly managed and initiate recovery action quickly.<br>4.13 To ensure sufficient preparedness in responding to cyber incidents detected, the FI must:<br>(a) identify scenarios of cyber risk that the FI is most likely to be exposed to;<br>(b) consider incidents in the capital market and the broader financial services industry;<br>(c) assess the likely impact of these incidents to the FIs; and<br>(d) identify appropriate response plan and communication strategies that should | Customers should continuously monitor for cyber incidents and breaches within its systems and network, establish a security incident escalation and decision-making processes, and undertake appropriate response plan and communication strategies. In addition, customers should also regularly conduct cyber security practical exercises to test the effectiveness of their response plans. Customers shall escalate to relevant personnel and implement appropriate responses when cyber breaches are detected. As a cloud service provider:<br>**(1)** HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. 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. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices.<br>**(2)** HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | be undertaken.<br>4.14 The FIs must regularly test, review and update the identified cyber risk scenarios and response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber threats.<br>4.15 The FIs must ensure that cyber breaches detected are escalated to an incidence response team, management and the board, in accordance with the entity's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. | them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident.<br>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.<br>**(3)** HUAWEI CLOUD has formulated various specific contingency plans to deal with complex security risks in the cloud environment. Each year, HUAWEI CLOUD conducts contingency plan drills for major security risk scenarios to quickly reduce potential security risks and ensure cyber resilience when such security incidents occur. HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes. |
| 4.17-4.19 | cyber risk - recovery | 4.17 The FIs must ensure that all critical systems are able to recover from a cyber breach within the FI's defined recovery time objective in order to provide important services or some level of minimum services for a temporary period of time.<br>4.18 The FIs must identify the critical | Customers should determine the recovery time objective of critical systems, and formulate a comprehensive recovery plan to ensure the timely recovery of services. As a cloud service provider<br>**(1)** To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs.<br>Under the requirements of this framework, HUAWEI CLOUD carries |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | systems and services within its operating environment that should be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the FIs will require to return to full service and operations.<br>4.19 The FIs must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber breach. | 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.<br>**(2)** In order to meet customer compliance requirements, 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. The recovery strategy covers all aspects of spare sites, equipment, personnel, information systems, and third parties. |

# 12 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of SC Guiding Principles on Business Continuity

SC released *Guiding Principles on Business Continuity* on May 14, 2019. This policy set FIs' business continuity management requirements from the perspectives of major operational disruptions, recovery objectives and strategies, testing and training, maintenance and review, communications and other domains.

When FIs are seeking to comply with the requirements provided in *Guiding Principles on Business Continuity*, 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 *Guiding Principles on Business Continuity*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| Business Continuity Guide Principle 2 | Major Operational Disruptions | Major operational disruptions and risks arising from interdependency and concentration of critical business functions as well as outsourcing arrangements should be identified. Any adverse impacts and implications of risks from such disruptions are thoroughly assessed and analyzed. | Customers should establish business impact analysis and risk assessment mechanism. As a cloud service provider:<br>**(1)** 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.<br>**(2)** HUAWEI CLOUD regularly conducts |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | risk assessment according to the requirements of the internal business continuity management system, identifies and analyses the potential risks faced by key resources supporting the continuous operation of cloud services, further considers emergency scenarios and risks, and formulates crisis management procedures to deal with and minimize the impact of various emergencies. Crisis management procedures include early warning and reporting of emergencies, emergency escalation, the conditions for starting emergency plans, notification of event progress, and internal and external communication processes. |
| Business Continuity Guide Principle 3 | Recovery Objectives and Strategies | Recovery objectives and strategies are developed according to risk-based principles where prioritization of recovery are based on the degree or level of risk the entity's business units poses to the entire business operation. | Customers should consider developing recovery strategies based on the results of business impact analysis and risk assessment. As a cloud service provider, 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. The restoration strategy takes site, equipment, personnel, information systems, third party and other aspects into consideration. |
| Business Continuity Guide Principle 4 | Communications | Comprehensive escalation procedures and communication plans during major operational disruptions for internal and external stakeholders are established and embedded in the business continuity framework. Such procedures should enable timely, transparent and coordinated dissemination of information that are adequate to address any reputational risks arising from major operational | Customers should establish communication mechanism with internal and external stakeholders. As a cloud service provider:<br>**(1)** HUAWEI CLOUD will actively cooperate regarding the communication initiated by the recognized authorities. HUAWEI CLOUD professional service engineer team provides 24/7 service support, customers can contact HUAWEI CLOUD support team through work orders, intelligent customer service, self-service, and hotline.<br>**(2)** HUAWEI CLOUD has also formulated crisis communication strategies according to the requirements of internal business continuity management system, and defined the people to contact in the case of emergencies, the dialogue, and the method for communication. |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | disruptions. | **(3)** To meet the requirements for notification, HUAWEI CLOUD has developed a complete process for event management and notification. If an event occurs on the HUAWEI CLOUD Base Platform, relevant personnel will analyze the impact of the event according to the process. If the event has or will have an impact on the cloud service customers, HUAWEI CLOUD will start to notify customers of the event. The contents of the notice include but are not limited to description of the event, the cause, impact, measures taken by HUAWEI CLOUD, and measures recommended for customers. The internal customer notification process ensures that HUAWEI CLOUD can promptly notify customers of events with an announcement when serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers. |
| Business Continuity Guide Principle 5 | Testing and Training | Testing and training are done at least annually by the FIs to ensure ongoing reliability and relevancy, incorporating evolving market practices, changes in key personnel and technology utilized in day-to-day business operations as well as regulatory policy updates. | Customers should establish a testing and training of business continuity plan mechanism. As a cloud service provider, HUAWEI CLOUD will actively cooperate regarding customer-initiated test requirements and help customers test the effectiveness of their business continuity plans.<br>HUAWEI CLOUD tests the business continuity plans and disaster recovery plans annually according to the requirements of the internal business continuity management system. All emergency response personnel, including reserve personnel, need to participate. The tests include desktop exercises, functional exercises and full-scale exercises, in which high-risk scenarios are emphasized. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After the completion of the test, relevant personnel write the test report and summarize any problems found during the test. If the test results show problems with the business continuity plan, recovery strategy or emergency |

| No. | Control Domain | Specific Control Requirements | HUAWEI CLOUD Response |
|---|---|---|---|
| | | | plan, the documents will be updated. |
| Business Continuity Guide Principle 6 | Maintenance and Review | The approach or framework for business continuity are regularly maintained and reviewed by FIs. Any material updates or changes are acknowledged, approved and endorsed by the Board and senior management. Employees are encouraged to be made aware of such updates or changes. | Customers should consider regular maintenance and review of business continuity plan. As a cloud service provider, HUAWEI CLOUD regularly reviews and updates all system documents every year according to the requirements of the internal business continuity management system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes.<br>Multiple copies of documents such as the business continuity plan, emergency response plan and disaster recovery operation manual are stored both electronically and in paper form and are distributed to relevant management and other key personnel. |

# 13 Conclusion

This Whitepaper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in Malaysia and shows that HUAWEI CLOUD complies with key regulatory requirements issued by Bank Negara Malaysia (BNM) and Securities Commission Malaysia (SC). This aims to help customers learn more about HUAWEI CLOUD's compliance status with Malaysia 's regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this Whitepaper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of Bank Negara Malaysia (BNM) and Securities Commission Malaysia (SC) on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This Whitepaper is for reference only and does not have any legal effect or constitute any legal advice. Customers should assess their own use of cloud services as appropriate and be responsible for ensuring compliance with relevant regulatory requirements from Bank Negara Malaysia (BNM) and Securities Commission Malaysia (SC) when using HUAWEI CLOUD.

# 14 Version History

| Date | Version | Description |
|---|---|---|
| 2024-7 | 2.1 | Routine update |
| 2023-2 | 2.0 | Compliance requirement update |
| 2022-4 | 1.1 | Routine update |
| 2020-9 | 1.0 | First release |