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

Issue 01

Date 2020-09-30

HUAWEI 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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.
- **Guidelines on Business Continuity Management**: This policy document sets out minimum Business Continuity Management (BCM) requirements on FIs so as to ensure the continuity of critical business functions and essential services within a specified timeframe in the event of a major disruption. Minimum disruption to essential business services would in turn enhance public confidence in FIs and the financial system, and mitigates reputational risk to FIs.

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).

2 HUAWEI CLOUD Security and Privacy Compliance

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

HUAWEI CLOUD has attained the following certifications:

Global standard certification

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

Certification	Description
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict 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.

Certification	Description
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
M&O certification	Uptime Institute is a globally recognized data center standardization organization and an authoritative professional certification organization. Huawei cloud data centers have obtained the M&O certification issued by Uptime Institute. The 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.
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.

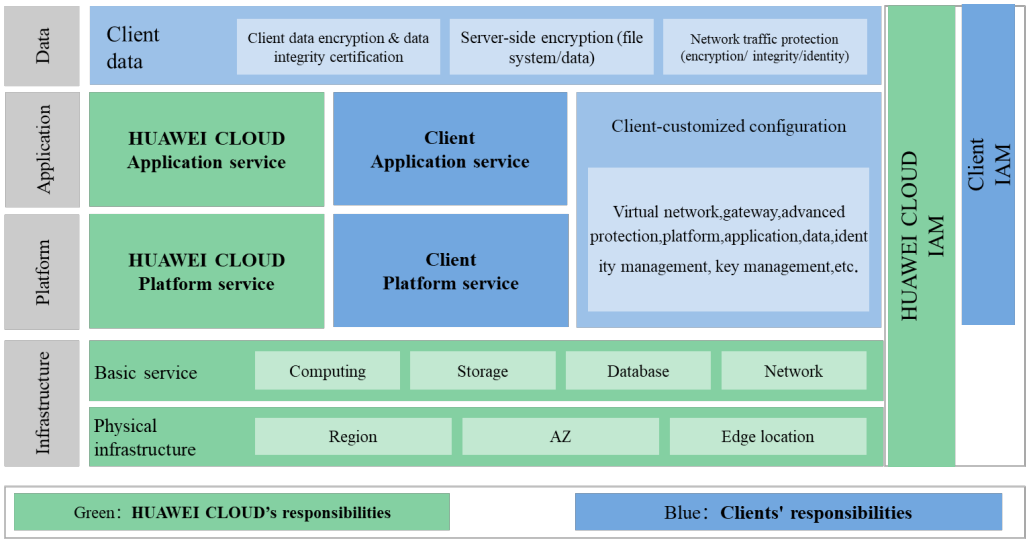
Certification	Description
Cloud Service Security Certification - Cyberspace Administration of China (CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD 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 - Security 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 customer and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help customers to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the customer and HUAWEI CLOUD:

Figure 3-1 Responsibility Sharing Model



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

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

and data layers, in addition to the identity and access management (IAM) cross-layer function.

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

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

4 HUAWEI CLOUD Global Infrastructure

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

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

BNM released *Risk Management in Technology* on July 18, 2019. 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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.5, 10.6, 10.7, 10.8, 10.10, 10.12, 10.13, and 10.14	System Development and Acquisition	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, 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. 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. 10.7 A FI shall consider the need for diversity in technology to	Customers should establish a security development management mechanism, and establish clear risk management policies and 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. As a cloud service provider: **(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 processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks. 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 prevent their unauthorized disclosure are in place. 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. 10.12 A FI shall physically segregate the production environment from the development and testing	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. **(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. **(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 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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. 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. 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 providers provide sufficient notice to the FI before any changes are undertaken that may impact the IT systems.	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. HUAWEI CLOUD has also developed a standardized emergency change management process. If emergency changes affect users, they will communicate with users in advance by announcement, mail, telephone, conference, or other means according to the prescribed time limit. If the emergency changes do not meet the prescribed notice time limit, the changes will be upgraded to HUAWEI CLOUD senior leadership, and users will be notified promptly after the changes are implemented. Emergency changes are recorded. The old version and data of the program are retained before the changes are executed. The changes are guaranteed to proceed smoothly through two-person operation to minimize the impact on the production environment. After the implementation, a designated person will verify it to help the change achieves its desired purpose.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.16, 19.19, and 10.20	Cryptography	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. 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 undertaken in a protected environment,	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. In order to cooperate with customers to meet regulatory requirements: **(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. **(2)** Currently, services including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		supported by a hardware security module (HSM) or trusted execution environment (TEM). 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.	provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.21-10.24	Data Center Resilience - Data Center Infrastructure	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. 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. 10.23 In addition to the requirement in paragraph 10.22 large FIs are also required to ensure recovery data centers are concurrently maintainable. 10.24 A FI shall host critical systems in a dedicated space intended for production data	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 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. As a cloud service provider, HUAWEI CLOUD will cooperate with customers to meet regulatory requirements from the following perspectives: **(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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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 and indicators of potential issues.	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. **(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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.26, 10.27, and 10.30	Data Center Resilience - Data Center Operations	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. 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. 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-	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. In order to cooperate with customers to meet regulatory requirements: **(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. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		controlled backup site.	**(3)** HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of **Object Storage Service (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 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.33, 10.34, 10.35, 10.36, 10.38, and 10.39	Network Resilience	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. 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. 10.35 A FI must establish real-time network bandwidth monitoring processes 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. 10.36 A FI must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	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, appropriate network isolation and other measures. As a cloud service provider: **(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. **(2)** 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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		10.38 A FI must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years. 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.	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. **(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. **(4)** In view of the scenario of hybrid cloud deployment and global layout of customer services, we 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. Among them, 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 between multiple local data centers

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and multiple cloud VPCs, support the interconnection of cross-cloud VPCs, and greatly improve the security and speed of global expansion of customer services. **(5)** 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 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. 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. **(6)** Customers can use the **Virtual Private Cloud (VPC)**, **Elastic Load Balance (ELB)** to network isolation and load balancing between different regions. Among them, the VPC service provided by HUAWEI CLOUD for

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.42, 10.43, 10.46, 10.47, and 10.48	Third Party Service Provider Management	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: (a) data leakage such as unauthorized disclosure of customer and counterparty information; (b) service disruption including capacity performance; (c) processing errors; (d) physical security breaches; (e) cyber threats; (f) over-reliance on key personnel; (g) mishandling of confidential information pertaining to the FI or its customers in the course of transmission, processing or storage of such information;	Customers should conduct due diligence on service providers' competency, system infrastructure and financial viability and capabilities in managing risks before selecting them. 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. In order to cooperate with customers to meet regulatory requirements: **(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. **(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. **(3)** HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		(h) concentration risk. 10.43 A FI must establish service-level agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following: (a) access rights for the regulator and any party appointed by the FI to examine any activity or entity of the FI. (b) requirements for the service provider to provide sufficient prior notice to FIs of any sub-contracting which is substantial; (c) a written undertaking by the service provider on compliance with secrecy provisions under relevant legislation; (d) arrangements for disaster recovery and backup capability, where applicable; (e) critical system availability; and (f) arrangements to secure business continuity in the event of exit or termination of the service provider. 10.46 A FI must ensure data residing	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. 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 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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-incident. 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. 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.	file storage all take customer data isolation as an important feature. **(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 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. When the service agreement terminates, customers can migrate 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.51 and 10.53	Cloud Services	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: (b) the availability of independent, internationally recognized certifications of the cloud service providers, at a minimum, in the following areas: (i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and (ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in	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 services. As a cloud service provider: **(1)** HUAWEI CLOUD has received a number of international and industry security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, CSA STAR, etc. 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. **(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. In addition, HUAWEI CLOUD service products and components have planned and implemented appropriate isolation mechanism from the beginning of design, avoiding unauthorized access

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		use, in storage and in transit. 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.	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. **(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. **(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 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			See section 6.8.2 Data Encryption Workshop (DEW) of ***HUAWEI CLOUD Security White Paper*** for more information.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.54, 10.56, 10.57, and 10.58	Access Control	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. 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 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).	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. In order to cooperate with customers to meet regulatory requirements: **(1)** Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Each HUAWEI CLOUD customer has a unique user ID in HUAWEI CLOUD, and provides a variety of user authentication mechanisms. • 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. • 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 authentication. MFA is used by default for changing important or sensitive account information

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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. 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.	such as passwords or mobile phone numbers. • 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. **(2)** 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. **(3)** 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 different responsibilities in different positions are limited to access the equipment under their role.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.65	Patch Management	A FI must establish a patch management framework which addresses among others the following requirements: (a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches; (b) conduct of compatibility testing for critical patches; (c) specification of turnaround time for deploying patches according to the severity of the patches; and (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. As a cloud service provider: **(1)** HUAWEI CLOUD **Image Management Service (IMS)** provides simple and convenient self-service management functions for images. Customers can manage their images through the IMS API or the management console. HUAWEI CLOUD staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to refer in deployment testing, troubleshooting, and other O&M activities. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 customers' services.

5.2 Cyber Security Management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.7-11.9	Cybersecurity Operations	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. 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. 11.9 A FI must conduct annual intelligence-led penetration tests on its internal and external network infrastructure as	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. In order to cooperate with customers to meet regulatory requirements: **(1)** 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 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. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		well as critical systems including web, mobile and all 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.	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. **(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 impact on clients' services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.13	Distributed Denial of Service (DDoS)	A FI must ensure its technology systems 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: (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; (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 (c) implementing mechanisms to mitigate against Domain Name Server (DNS) based layer attacks.	Customers should 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. In order to cooperate with customers to meet regulatory requirements: 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. **(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. **(3)** HUAWEI CLOUD Anti-DDoS attack services also leverages other

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.15	Data Loss Prevention (DLP)	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 technology deployed must cover the following: (a) data in-use – data being processed by IT resources; (b) data in-motion – data being transmitted on the network; and (c) data at-rest – data stored in storage mediums such as servers, backup media and databases.	Customers should establish a data leakage prevention mechanism and use appropriate technical means to prevent data leakage. The deployed technology should cover the data life cycle of data usage, data transmission, and data storage. 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: **(1) Data creation**: HUAWEI CLOUD provides services on a regional basis, which is the storage location of customer content data. HUAWEI CLOUD will never 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			keys to decrypt data, which supports data security on the cloud. **(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. For more information, please refer to Section 4.5 of "Whitepaper for HUAWEI CLOUD Data Security". **(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 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. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(6) Data destroying: If customers want to delete data or data needs to be deleted due to the expiration of a service, HUAWEI CLOUD strictly follows the data destruction standard and agreement with customers to clear the stored data.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.17	Security Operations Center (SOC)	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 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.	Customer should establish SOC to detect user or network activities, identify breaches and establish the appropriate response. As a cloud provider: **(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 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. See section 8.3 Security Logging & Event Management of ***HUAWEI CLOUD Security White Paper*** for more information.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.22-11.25	Cyber Response and Recovery	11.22 A FI must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the 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. 11.23 A FI must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). 11.24 A FI must ensure that relevant Cyber Emergency Response Team (CERT) members are conversant with the incident response plan and handling procedures, and remain contactable at all times.	Customers should establish cyber crisis management policies and procedures, establish and implement a 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. As a cloud service provider: **(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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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.	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. **(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 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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
12.5	Technology Audit	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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
13.1-13.4	Internal Awareness and Training	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. 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. 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	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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		cloud operations are also suitably certified. 13.4 A FI must provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.	and enablement, on boarding qualifications management, off boarding security review. See section 4.4 Human Resource Management of ***HUAWEI CLOUD Security White Paper*** for more information.

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

BNM released *Outsourcing* onOctober 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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.3	Assessment of Service Provider	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. The due diligence process must cover, at a minimum: (a) capacity, capability, financial strength and business reputation; (b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management; (c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites; (d) access rights of the FI and the Bank to the service provider;	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 technical capabilities, financial resources, business reputation, risk management capabilities, location of outsourcing activities, data security, reliance on subcontractors, etc. As a cloud service provider, HUAWEI CLOUD's performance in the aforesaid aspects is as follows: **(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 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		(e) measures and processes to ensure data protection and confidentiality; (f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement; (i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document.	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. **(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. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. **(4)Operational capability:** HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. **(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. **(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 document. **(7) Data security**: Please refer "Data Confidentiality Protection" in section 6.1 "Outsourcing Process and Management of Risks" of this document. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. **(9)Corporate culture and service policies suitable for FIs:** HUAWEI CLOUD defines product safety and functional 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.6 and 9.7	Outsourcing Agreement	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. 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 the Bank deems necessary; (c) enable the Bank to appoint an independent party to perform a review of the relevant systems,	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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.8 and 9.9	Protection of Data Confidentiality	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. 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: (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 comparable to Malaysia; (e) where the service provider provides services to multiple clients, the FI's information must be segregated 18 from the	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: **(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 sustainable security infrastructure and services to our customers. We will also openly and transparently 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		information of other clients of the service provider; (f) the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even after the arrangement has ceased; and (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.	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. **(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. **(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. **(4)** When the service agreement terminates, customers can migrate 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. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.10, 9.13, and 9.14	Business Continuity Planning	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. 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. 9.14 A FI must periodically test its own BCP and proactively seek assurance on the 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:	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 service providers test their business continuity plans and make continuous improvements. To meet regulatory requirements, HUAWEI CLOUD cooperates with customers : **(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. **(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. 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		(a) ensure that the back-up arrangements are available and ready to be operated when necessary; (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 (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.	business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. **(4)** 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. HUAWEI CLOUD tests the BCPs 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 BCPs, recovery strategy or emergency plan, the documents will be updated.

6.2 Outsourcing Outside Malaysia

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.1-10.3	Outsourcing Outside Malaysia	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. 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 provider to implement appropriate responses to emerging risk events in a timely manner. 10.3 A FI must ensure that outsourcing	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 business development and regulatory requirements. 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, 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		arrangements undertaken outside Malaysia are conducted in a manner which does not affect: (a) the FI's ability to effectively monitor the service provider and execute the institution's BCP; (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 (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.	

6.3 Outsourcing Involving Cloud Services

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.3 and 11.4	Outsourcing involving Cloud Services	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 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. 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	Customers should regularly review cloud service providers, or obtain third-party certification and reports. In addition, customers should also obtain information about business continuity management of the cloud service providers. 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 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. 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		arising from the BCP testing.	

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

BNM released *Management of Customer Information and Permitted Disclosures* on October 17, 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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.1 and 10.2	Risk Assessment	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. 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.	Customers should identify potential security threats and vulnerabilities, and assess the likelihood that such threat and vulnerability, as well as the potential impact caused by security incidents. 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 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.6 and 10.11	Policies and Procedures	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. 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 environment.	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 activities every year to identify problems in the operation of the system each year and rectify them to continuously improve the management system.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.12, 10.13, 10.20, and 10.21	Control Measures - Information and Communication Technology (ICT) Controls	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. 10.13 FSPs must regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats. 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. 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	Customers should deploy preventive and detective ICT controls, regularly monitor the effectiveness of these controls, and establish an accountability mechanism for information disclosure. In order to cooperate with customers to meet regulatory requirements: **(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. 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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		unauthorized disclosure by whatever means, installing CCTV at 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.	Fortress Machine to realize the deep audit of user login. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(3) HUAWEI CLOUD data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.26 and 10.27	Access Controls	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. 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. In order to cooperate with customers to meet regulatory requirements: **(1)** Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. 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. **(2)** 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. **(3)** HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.28, 10.29, and 10.32	Physical Security	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. 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. 10.32 To effectively safeguard customer information throughout its lifecycle, FSPs must 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	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: **(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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and digital records of the customer information.	safety of HUAWEI CLOUD data centers. **(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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.39, 10.40, 10.42, 10.43, 10.44, 10.45, 10.49, and 10.50	Staff, Representatives, Agents and External Vendors' Personnel	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 requirement of any written law to safeguard customer information as well as the consequences for failure to comply with such obligation and requirement. 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. 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.	Customers should require all staff to sign a confidentiality undertaking that clearly specifies the obligation and requirement of safeguard 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. As a cloud service provider: **(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 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. **(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. **(3)** HUAWEI CLOUD provides online version of ***HUAWEI CLOUD Customer Agreement*** and ***HUAWEI CLOUD Service Level Agreement***,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		10.43 FSPs must provide relevant training and regularly remind all staff on their obligations to properly handle customer information. 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. 10.45 New staff must also be alerted by the FSPs on the possible actions that may be taken for non-compliance with policies and procedures. 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. 10.50 The actions taken pursuant to paragraph 10.49 must send a strong message to all staff	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. **(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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and act as deterrent to prevent future recurrence of the customer information breach.	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.
10.53	Independent Review	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 protection certifications, and is audited by third party every year.

7.2 Customer Information Breaches

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.12, and 11.13	Customer Information Breaches	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. 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. 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. 11.4 FSPs must have in place a mechanism to	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: **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		identify customer information breaches including those which arise from customer complaints and investigate the complaints promptly and properly. 11.5 FSPs must take appropriate mitigating actions to contain a customer information breach immediately. 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. 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. 11.13 The actions referred to in paragraph 11.12 may include the following: (a) making a public announcement to notify the	to communicate alert logs for unified analysis of a variety of security devices. **(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. 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. **(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. If the results are indicating issues with the information security incident management and process, related

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		customers promptly to regain customers' confidence; (b) providing contact details for customers to obtain further information or raise any concern with regard to the breach; or (c) providing advice to affected customers on protective measures against potential harm that could be caused by the breach.	documentation will be accordingly updated. 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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
12.2, 12.3, 12.4, 12.6, and 12.7	Outsourced Service Provider (OSP)	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. 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 properly safeguarded at all times. 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: (a) undertake to safeguard the customer information and prevent any theft, loss, misuse or	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 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. In order to cooperate with customers to meet regulatory requirements: **(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 recovery. Inviolable ownership and control are necessary to provide users with the effective data protection. In addition, HUAWEI CLOUD has formulated an

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		unauthorized access, modification or disclosure by whatever means; (b) ensure the adequacy and effectiveness of its policies and procedures to protect the FSP's customer information; (c) conduct robust vetting on its personnel who handles customer information; (d) only allow its personnel access to customer information strictly for the purpose of carrying out their functions; (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 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); (f) investigate any customer information breach	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. **(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. **(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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		to determine when and how the breach occurred; (g) report any customer information breach to the FSP within an agreed timeframe; (h) destroy in accordance with paragraph 10.32 or return all customer information to the FSP upon the expiry or termination of the SLA; (i) allow the FSP to audit or inspect how customer information is safeguarded. 12.6 FSPs must require the OSP to sign a binding non-disclosure undertaking with regard to the handling of customer information. 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 adequacy and effectiveness of the training program.	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. **(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.

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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.12	Principle 2 - Data Governance	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.
4.14(VI)	Principle 3 - Data Architecture	The FI should establish 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.	Please refer to the control domain of **"Data Center Resilience - Data Center Operations"** under **5.1 Technology Operations Management** of this document.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.20, 4.23, 4.25, and 4.27	Principle 5 - Internal Controls and Reviews	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. 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. 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	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 Domain	Specific Control Requirements	HUAWEI CLOUD Response
		for services contracted should clearly prohibit the unauthorized disclosure of confidential data by the external party and provide for adequate remedies to the FI. 4.27 Appropriate safeguards should be put in place to ensure that personal data is not misused or disclosed in a wrongful manner. Personal 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 Guidelines on Business Continuity Management

BNM released *Guidelines on Business Continuity Management* on January 1, 2008. This policy set FIs' customer business continuity management requirements in the perspectives of the principles and requirements of business continuity management (BCM), communication, internal audit, outsourcing and other domains.

When FIs are seeking to comply with the requirements provided in *Guidelines on 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 *Guidelines on Business Continuity Management*, 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
71	BCM Principles and Requirements-Methodology-Alternate and Recovery Sites	The alternate and recovery sites could either be in-house arrangements, or available through agreement with third-party recovery facility provider, or a combination of both options.	Please refer to the control domain of **"Outsourcing Agreement"** under **6.1 Outsourcing Process and Management of Risks** of this document.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
109-114	Outsourcing	109. The FI should ensure that the outsourcing vendor is subjected to the BCM Guidelines, where appropriate. 110. The outsourcing contract should specify the requirements for ensuring the continuity of the outsourced business function in the event of a major disruption affecting the outsourcing vendor's services. Recovery time objectives (RTO) should be built into the outsourcing contract, with provisions for legal liability should the RTO not be achieved. 111. The FI should ensure that the outsourcing vendor has in place fully documented and adequately resourced business continuity plan (BCP) and disaster recovery plan (DRP). The institution should ensure that periodic testing is conducted by the outsourcing vendor on its BCP and DRP at least annually and twice a year, respectively. The	Please refer to the control domain of **"Outsourcing Agreement"** and **"Business Continuity Planning"** under **6.1 Outsourcing Process and Management of Risks** of this document.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		vendor should notify the FI of the test results and action to be undertaken to address any gap. The FI may also require its outsourcing vendor to declare their state of business continuity readiness to the institution, annually. 112. The FI should include a clause in the outsourcing agreement, which allows the institution's internal auditor or other independent party appointed to review the BCM of the outsourcing vendor. 113. The FI should be notified in the event that the outsourcing vendor makes significant changes to its BCP and disaster recovery plan (DRP), or encounters other circumstances that might have a serious impact on its services. 114. The FI's own BCP should address reasonably foreseeable situations where the outsourcing vendor fails to provide the	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		required services, causing disruptions to the FI's operations. In particular, the plan should ensure that the FI has in its possession, or can readily access, all records necessary for it to sustain business operations and meet obligations in the event the outsourcing vendor is unable to provide the contracted services.	

10 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. 4.6 The assessment of the vulnerabilities of FI's operating environment must be 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. 4.7 The FI must develop and implement preventive measures to minimize the FI's exposure to cyber risk. 4.8 Preventive measures referred to in Paragraph 4.7	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: **(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-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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		above may include the following: (a) Deployment of anti-virus software and malware program to detect and isolate malicious code; (b) Layering systems and systems components; (c) Build firewalls to reduce weak points through which attacker can gain access to an entity's network; (d) Rigorous testing at software development stage to limit the number of vulnerabilities; (e) Penetration testing of existing systems and networks; and (f) Use of authority matrix to limit privileged internal or external access rights to systems and data. 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,	vulnerability exploitation related service impacts to our customers. **(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. **(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 centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		incidents and scenarios. 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.	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. **(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. **(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 employee behavior complies with all applicable laws, policies, processes and requirements in Huawei's business code of conduct.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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. 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. 4.13 To ensure sufficient preparedness in responding to cyber incidents detected, the FI must: (a) identify scenarios of cyber risk that the FI is most likely to be exposed to; (b) consider incidents in the capital market and the broader financial services industry; (c) assess the likely impact of these incidents to the FIs; and (d) identify appropriate	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: **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		response plan and communication strategies that should be undertaken. 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. 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.	unified analysis of a variety of security devices. **(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. 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. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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. 4.18 The FIs must identify the critical 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. 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.	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 **(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. 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. **(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.

11 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: **(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. **(2)** HUAWEI CLOUD regularly conducts risk assessment according to the requirements of the internal business continuity management system, identifies and analyses the potential risks faced by key 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 disruptions.	Customers should establish communication mechanism with internal and external stakeholders. As a cloud service provider: **(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. **(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. **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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. 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 plan, the documents will be updated.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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. 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.

12 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.

13 Version History

Date	Version	Description
2020-09-30	1.0	First release

