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

Issue	**3.0**
Date	**2024-01-26**

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

In the recent wave of technological development, more and more financial institutions (FIs) are seeking to transform their business. They want to leverage advanced technology to reduce costs, improve operational efficiency, and innovate their business model. To standardize the application of the Information Technology (IT) in the financial Industry, the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) have published a series of regulatory requirements, guidelines and notices. These requirements address risk management of Singapore FIs towards outsourcing management and cloud computing implementation.

HUAWEI CLOUD, as a cloud service provider, is committed to helping FIs meet these regulatory requirements and continuously provide financial customers with cloud services and business operating environments that meet FI standards. Currently, HUAWEI CLOUD has established a methodology that covers mainstream cloud security standards and HUAWEI CLOUD security management requirements in the industry, covering multiple aspects of cyber security and privacy protection requirements. The implementation of the methodology helps improve HUAWEI CLOUD's compliance level. At the same time, it can assist financial clients in meeting relevant regulatory requirements, guidelines and notices.

The article details how HUAWEI CLOUD will assist Singapore FIs in meeting regulatory requirements for cloud services:

- **MAS Guidelines on Outsourcing**: Set out the MAS expectations of an FI that has entered into any outsourcing arrangement or is planning to outsource its business activities to a service provider. The Guidelines provide guidance on sound practices on risk management of outsourcing arrangements.
- **MAS Technology Risk Management Guidelines**: Set out risk management principles and best practice standards to guide the FIs in establishing a sound and robust technology risk management framework.
- **MAS Notice on Cyber Hygiene**: Provide FIs in Singapore with practical guidance on compliance with relevant acts.
- **ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers**: Stipulate the minimum/baseline controls that outsourced service providers which wish to service the FIs should have in place.
- **ABS Cloud Computing Implementation Guide**: Sets out best practices and considerations for FIs on using cloud services.
- **MAS Business Continuity Management Guidelines**: provides guidance for FIs in Singapore to strengthen business continuity management and aims to help FIs increase their resilience to service disruptions while minimizing the negative impact of service disruptions.

- **MAS Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption:** This advisory highlight some of the more common key risks and control measures that FIs should consider before adopting public cloud services, providing guidance for FIs to use public cloud services more securely and reduce related risks.

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 global, regional, and industry-specific security compliance certifications ensuring the security and compliance of businesses deployed by cloud service customers.

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

Example of Huawei Cloud Partial Standard Certification:

Certification	Description
ISO27001:2022	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.
ISO27017:2015	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.
ISO27018:2019	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.
TL 9000& ISO 9001	ISO 9001 defines a set of core standards for quality management systems (QMS). It can be used to certify that an organization has the ability to provide products that meet customer needs as well as applicable regulatory requirements. TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers

Certification	Description
	and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000. Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.
ISO 20000-1:2018	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.
ISO22301:2019	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	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, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
ISO27701:2019	ISO 27701 specifics 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.
ISO29151:2017	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.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.

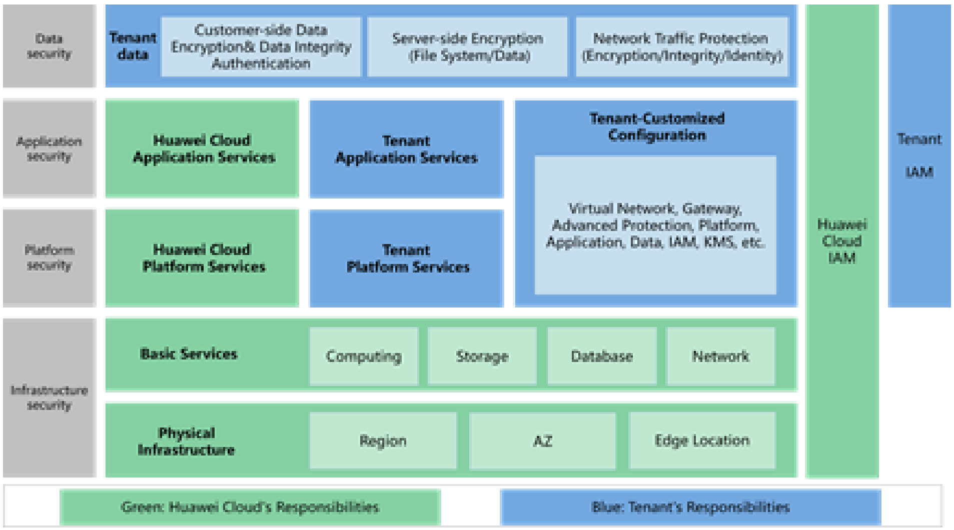
Certification	Description
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.
ISO 27799:2016	ISO/IEC 27799 provides guidelines on how organizations in the healthcare industry can better protect the confidentiality, integrity, traceability, and availability of personal health information. Huawei Cloud is the world's first cloud service provider to earn ISO/IEC 27799 certification. This certifies Huawei Cloud's deep understanding of intelligent applications for the healthcare industry, and its ability to protect the security of personal health information.
ISO 27034	ISO/IEC 27034 is the first ISO standard for secure programs and frameworks. It clearly defines risks in application systems and provides guidance to assist organizations in integrating security into their processes. ISO/IEC 27034 provides a way for organizations to verify their own product security and make security a competitive edge. This standard also outlines a compliance framework at the application layer for global cloud service providers, promoting the security of the R&D process, applications, and the cloud. Huawei Cloud is the world's first cloud service provider to obtain ISO/IEC 27034 certification. This marks a big step forward for Huawei Cloud governance and compliance.
SOC Audit Report	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.

3 HUAWEI CLOUD Security Responsibility Sharing Model

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.

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

Figure 3-1 Responsibility Sharing Model


Data security
Tenant data
Customer-side Data Encryption& Data Integrity Authentication
Server-side Encryption (File System/Data)
Network Traffic Protection (Encryption/Integrity/Identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Tenant-Customized Configuration
Virtual Network, Gateway, Advanced Protection, Platform, Application, Data, IAM, KMS, etc.
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
Basic Services
Computing
Storage
Database
Network
Physical Infrastructure
Region
AZ
Edge Location
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's Responsibilities
Blue: Tenant's Responsibilities

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

4 HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZ 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 Can Help Customers to Meet the Requirements of MAS Guidelines on Outsourcing

From the perspective of risk management, the *Guidelines on Outsourcings*[2] elaborate matters that FIs need to consider and requirements they should comply with when they are engaged in outsourcing. The MAS Outsourcing Guidelines covers Engagement with MAS on Outsourcing, Risk Management Practices and Cloud Computing. It also expresses the expectations of MAS on the outsourcing management of FIs.

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

5.1 Engagement with MAS on Outsourcing

Chapter 4 of the *Guidelines on Outsourcing* requires FIs to continuously engage with MAS to demonstrate its observance of these guidelines. Requirements cover Observance of the Guidelines and Notification of Adverse Developments. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.1	Observance of the Guidelines	An institution should be ready to demonstrate to MAS its observance of these guidelines. MAS may directly communicate with the home or host regulators of the institution and the institution's service provider, on their ability and willingness to cooperate with MAS in supervising the outsourcing risks to the institution.	Customers should conduct audit or assessment of their outsourced service providers on a regular basis, to ensure that service providers provide cloud services under the premise of not less stringent than their own security management
4.2	Notification of Adverse Developments		

			requirements. If an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange for someone to actively cooperate with the audit.

5.2 Risk Management Practices

Chapter 5 of the *Guidelines on Outsourcing* requires FIs to formulate risk management policies for outsourcing arrangements and to comply with relevant practices of outsourcing risk management. Requirements cover Overview, Responsibility of the Board and Senior Management, Evaluation of Risks, Assessment of Service Providers, Outsourcing Agreement, Confidentiality and Security, Business Continuity Management, Monitoring and Control of Outsourcing Arrangements, Audit and Inspection, Outsourcing Outside Singapore, Outsourcing Within a Group and Outsourcing of Internal Audit to External Auditors. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.3	Evaluation of Risks	In order to be satisfied that an outsourcing arrangement does not result in the risk management, internal control, business conduct or reputation of an institution being compromised or weakened, The FI should establish a framework for risk evaluation. Such risk evaluations should be performed when an institution is planning to enter into an outsourcing arrangement with an existing or a new service provider, and also re-performed periodically on existing outsourcing arrangements, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the institution.	Customers should establish a risk assessment framework to regularly assess the risks of outsourcing arrangements. HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment.
5.4	Assessment of Service Providers	In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due	Customers should conduct due diligence to identify the risks of their outsourcing arrangements with service providers. HUAWEI CLOUD will assign

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		diligence processes to assess the risks associated with the outsourcing arrangements. Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, The FI should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the institution's hiring policies for the role they are performing.	special personnel to actively cooperate with this due diligence by customers. HUAWEI CLOUD has constructed a complete security system from security technology, security system, personnel management and other aspects in accordance with the most authoritative security standards in all regions of the world, and has obtained numerous security certifications at home and abroad. This allows users to enjoy a secure and trustworthy cloud platform and cloud services. Huawei advocates company-wide for a mindset and practice wherein "everyone understands security", cultivating a security culture that is present 24/7, as well as dynamic and competitive throughout the company. The impact of such a culture runs through talent recruitment, new-hire orientation, initial and ongoing training, internal transfer, and internal re-training, all the way up to employment termination.
5.5	Outsourcing Agreement	Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements. They should also be vetted by a competent authority (e.g., the institutions' legal counsel) on their legality and enforceability. An institution should ensure that every outsourcing agreement addresses the risks identified at the risk evaluation and due diligence stages. Each outsourcing agreement should allow for timely renegotiation and renewal to enable the	Customers and outsourced service providers should sign outsourcing agreements and ensure the legality and enforceability of the agreements. HUAWEI CLOUD cooperates with customers to exercise supervision over cloud service providers. The online *HUAWEI CLOUD Customer Agreement* defines cloud service customers and Huawei's security responsibilities, and the *HUAWEI CLOUD Service Level Agreement* stipulates the service level provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed a negotiable offline contract template to address

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations. Each agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore	specific customer needs. For more information, please refer to *HUAWEI CLOUD Customer Agreement.*
5.6	Confidentiality and Security	FIs must ensure that the security policies, procedures and controls of service providers will enable them to protect the confidentiality and security of their client information.	Customers can use agreement constraints, reviews, and other means to ensure the security policies, procedures, and controls of service providers enable organizations to protect the confidentiality and security of their customer information. The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and sustainable security infrastructure and services to our customers. We will also openly and transparently tackle cloud security challenges standing shoulder-to-shoulder with our customers and partners as well as relevant governments in order to meet all the security requirements of our cloud users. HUAWEI CLOUD has obtained many authoritative security and privacy protection certificates in the world. Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on HUAWEI CLOUD. For more details, please refer to *HUAWEI CLOUD Security White Paper*.
5.7	Business Continuity Management	FIs should ensure that its business continuity is not compromised by outsourcing arrangements, such that the institution remains able to conduct its business with integrity and competence in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider.	Customers should make business continuity plans and consider the impact of outsourcing arrangements on their business continuity. If FIs need HUAWEI CLOUD's participation in the running of business continuity plans within their organizations, HUAWEI CLOUD will actively cooperate. Additionally, HUAWEI CLOUD, as a cloud service provider, will provide FIs with cloud services to meet the needs of their business except when outsourcing is interrupted or unexpectedly terminated caused by force majeure. HUAWEI CLOUD has also developed a business continuity management system that is consistent with its own business characteristics to provide continuous and effective services to customers and ensure the development of customer business. HUAWEI CLOUD conducts internal business continuity publicity and training every year, including regular

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			emergency drills and tests, to continuously optimize emergency response.
5.8	Monitoring and Control of Outsourcing Arrangements	Establish outsourcing management control groups to monitor and control the outsourced service on an ongoing basis. Periodic reviews, at least on an annual basis, on all material outsourcing arrangements. Perform comprehensive pre- and post-implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements. If an outsourcing arrangement is materially amended, a comprehensive due diligence of the outsourcing arrangement should also be conducted.	Customers should establish mechanisms for outsourcing management, and continuously monitor and review their outsourced services. Customers can monitor the use and performance of their own cloud resources through HUAWEI CLOUD monitoring services **Cloud Eye Service (CES)**. HUAWEI CLOUD can also provide service reports according to SLA and customer needs. If FIs need to conduct inspection and due diligence on HUAWEI CLOUD and its operation, HUAWEI CLOUD will organize a dedicated person to assist.
5.9	Audit and Inspections	An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives. An institution should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. The outsourcing agreement should also include clauses that require the service provider to comply, as soon as possible, with any request from MAS or the institution, to the service provider and its sub-contractors to submit any reports on the security and control environment of the service provider and its sub-contractors, in relation to the outsourcing arrangement. Significant issues and concerns should be brought to the attention of the senior management of the institution	Customers should conduct an independent audit or expert assessment of their outsourced service providers on a regular basis and inform the service provider's senior management of identified issues. Customers should also require that the service provider's security commitment is included when signing with subcontractors. If an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange for someone to actively cooperate with the audit. Customer audit and supervision interests 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 parties every year.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and service provider, or to the institution's board, where warranted, on a timely basis. Actions should be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the institution's risk tolerance.	Additionally, HUAWEI CLOUD has developed a complete supplier management mechanism that regularly assesses the performance of suppliers (including outsourcing personnel). The results of the assessment are used as an important reference for the next procurement. HUAWEI CLOUD also has security compliance and confidentiality agreements with suppliers, including outsourced individuals.
5.10	Outsourcing Outside Singapore	The engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in a foreign country, may expose an institution to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, an institution should take into account, as part of its due diligence, and on a continuous basis: (a) government policies; (b) political, social, economic conditions; (c) legal and regulatory developments in the foreign country; and (d) the institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.	When choosing 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. 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 country, one customer, one policy" 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			challenges of cloud security and meet the security needs of customers in an all-round way. HUAWEI CLOUD has established two data centers in Singapore for dual AZ redundancy. To reduce service disruption struck by hardware failures, natural disasters, or other disasters, HUAWEI CLOUD provides a disaster recovery plan for all data centers: data center connectivity (DCI - Data Center Interconnect) across different availability zones in a single region. To meet the basic requirements of cross AZ data replication, users can select disaster preparedness replication services based on business requirements.
5.11	Outsourcing Within a Group	Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects of the service provider’s ability to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, audit and inspection, including confirmation on the right of access to be provided to MAS, to retain effective supervision over the institution, and compliance with local regulatory standards.	Customers should conduct due diligence on service providers before selecting them. Review whether the service provider's business continuity mechanism meets business requirements and negotiate so as to eventually agree with suppliers about the content of the contract. HUAWEI CLOUD will arrange for someone to actively cooperate with the customer during their inspection and due diligence. HUAWEI CLOUD will hire professional external resources to conduct SOC2 certification every year. If the customer demands more from the user agreement, HUAWEI CLOUD will try to reach an agreement. HUAWEI CLOUD will actively cooperate with MAS and FIs to audit HUAWEI CLOUD and its suppliers.

5.3 Cloud Computing

Chapter 6 of *Guidelines on Outsourcing* puts forward the matters needing attention and requirements that FIs should comply with when using cloud services. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6	Cloud Computing	When ordering cloud services, financial institutions should carry out necessary due diligence and take active measures to deal with risks related to data access, confidentiality, integrity, sovereignty, restorability, compliance and audit. Organizations should ensure that service providers can use strong physical or logical controls to clearly identify and isolate customer data. Service providers should establish reliable access controls to protect customer information, which should be used for the duration of the cloud service contract.	Before ordering cloud services, customers should conduct inspection and due diligence on cloud service providers, especially considering how cloud services control data access, confidentiality, sovereignty, recoverability and compliance, and how to achieve customer data isolation solutions in multi-tenant scenarios. 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 ensure the privacy of tenants' 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 most effective data protection. For more information, please refer to Part 4 of *White Paper for HUAWEI CLOUD Data Security*.

6 How HUAWEI CLOUD Can Help Customers to Meet the Requirements in MAS Technology Risk Management Guidelines

The *Technology Risk Management Guidelines 2021* issued by the MAS stipulate the management principles and best practice standards of financial institutions on technology risks, so as to guide Singapore's FIs to establish a sound and reliable scientific and technological risk management framework, as well as strengthen the security, reliability, flexibility and restorability of the system, and protect customer data, transactions and information systems. *Technology Risk Management Guidelines* 2021 covers Technology Risk Governance and Oversight, Technology Risk Management Framework, IT Project Management and Security-by-Design, Software Application Development and Management, IT Service Management, IT Resilience, Access Control, Cryptography, Data and Infrastructure Security, Cyber Security Operations, Cyber Security Assessment, Online Financial Services and IT Audit.

The following summarizes Technology Risk Management Guidelines 2021 and explains how HUAWEI CLOUD is assisting FIs to meet these requirements in the following control domains.

6.1 Technology Risks Governance and Oversight

Chapter 3 of the *Technology Risk Management Guidelines 2021* emphasizes the importance of IT functions in supporting the business of FIs, requiring the board of directors and senior management of FIs to monitor their technology risks and ensure that the IT functions of the organization support their business strategies and objectives. Requirements cover Role of the Board of Directors and Senior Management, Policies, Standards and Procedures, Management of Information Assets, Management of Third Party Services, Competency and Background Review and Security Awareness and Training. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.2	Policies, Standards and Procedures	Policies, standards and procedures, where appropriate, incorporate industry	Customers should establish and regularly review formal information security policies and processes. According to ISO 27001, HUAWEI

		standards and best practices to manage technology risks and safeguard information assets should be established. The policies, standards and procedures established should be regularly reviewed and updated to ensure it is still relevant to the evolving technology and cyber threat landscape.	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. In addition, HUAWEI CLOUD focuses on the development of security awareness among employees and outsourcing personnel, and has developed an applicable security awareness training program that is applied regularly.
3.3	Management of Information Assets	To have an accurate and complete view of its IT operating environment, FIs should establish information asset management practices. An inventory of all the information assets should be maintained, reviewed periodically and updated whenever there are changes.	Customers should conduct unified management of their information assets, which should indicate the classification of the corresponding assets and the physical location (country or region) where the data is stored, and identify the requirements for data retention and information security issued by the country or region. HUAWEI CLOUD provides customers with a unified management interface for customers to query and manage their purchased HUAWEI CLOUD resources. Customers can also use the asset management function of Huawei Cloud Host Security Service (HSS) for unified management of their assets.
3.4	Management of Third Party Services	The FIs should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and	Customers should conduct due diligence before selecting a service provider, especially in terms of governance, risk and compliance management mechanisms. Customers should develop a list of reputable

		availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.	service providers, and be able to identify whether there are any viable alternatives to the preferred service provider. HUAWEI CLOUD provides online version of HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence by FIs. Customers' 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 ISO27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.
3.5	Competency and Background Review	As people play an important role in managing systems and processes in an IT environment, the FI should implement a screening process that is comprehensive and effective.	Customers should develop and implement screening strategies and procedures for personnel. HUAWEI CLOUD conducts adequate background checks before hiring employees, including criminal records, financial irregularities, dishonest records, government background, experience in sanctioning countries, and whether to sanction citizens of a country. Simultaneously, in order to manage in an orderly way and reduce the potential impact of personnel management risks on business continuity and safety, HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers, including On-boarding security review, On-the-job security training and enablement, On-boarding qualifications management, Off-boarding security review.
3.6	Security Awareness and Training	All contractors and suppliers who have access to financial institution IT resources and IT systems should develop safety	To raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations, Huawei provides employee security awareness training in three ways: company-wide

		awareness training plans and implement or update them at least once a year.	awareness training, awareness promotion events, and the signing of BCG commitment agreements. Security awareness training is also conducted at least once a year for all employees.

6.2 Technology Risk Management Framework

Chapter 4 of the *Technology Risk Management Guideline 2021* requires FIs to establish a risk management framework to manage the technology risks. Requirements cover Risk management Framework, Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring, Review and Reporting. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.1	Risk Management Framework	The FI should establish a risk management framework to manage technology risk. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities and clear reporting lines across the various organizational functions.	Customers should establish a risk assessment framework to regularly assess the risks of outsourcing arrangements. HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment. HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts an annual risk assessment and increases the number of risk assessments for major changes in information systems, a significant change in the company's business, or a significant change in laws, regulations or standards. It also carries out strict security management for outsourcers, and regularly audits and evaluates its suppliers.

4.2	Risk Identification	The FI should identify the threats and vulnerabilities application to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	Customers should conduct risk assessments on their outsourced businesses and preferred service providers to identify potential risks. HUAWEI CLOUD develops and maintains an internal risk management framework to identify, analyze and manage risks that have been identified. A formal risk assessment is performed at least annually to determine the likelihood and impact of identified risks. Procedure is established to guide the Management for risk calculation and risk classification which determine the likelihood and impact of identified risks. The likelihood and impact associated with each risks is determined independently, considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by Management. Additionally, at least monthly, HUAWEI CLOUD organizes meetings to discuss the assessment on the risks which have been identified in relation to network security and privacy protection. Corresponding follow-up actions are taken and documented to ensure the risks have been managed appropriately based on Huawei's risk management requirements.
4.3	Risk Assessment	The FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.	
4.4	Risk Treatment	The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile.	
4.5	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	

6.3 IT Project Management and Security-by-Design

Chapter 5 of the *Technology Risk Management Guideline 2021* requires FIs to establish a project management framework to ensure consistency in project management practices. Requirements cover Project Management Framework, Project Steering Committee, System

Acquisition, System Development Life Cycle and Security-By-Design, System Requirements Analysis, System Design and Implementation, System Testing and Acceptance and Quality Management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	Response of HUAWEI CLOUD
5.1	Project Management Framework	A project management framework should be established to ensure consistency in project management practices, and delivery of outcomes that meets project objectives and requirements. Detailed IT project plans should be established for all IT projects which includes scope of the project, activities, milestones and the deliverables to be realized at each phase of the project.	Customers should establish a project management framework to ensure that the delivery and practice processes of the outsourced project meet their project objectives and requirements. For each IT project plan, customers should consider the project scope, activities, milestones, and what should be delivered at each stage. HUAWEI CLOUD has developed a complete project management approach and is CCM5/CMMI, ISO 9001:2000 and PMI framework based practices which have enabled successful project implementations over the world by qualified project and project management professionals.
5.3	System Acquisition	FIs should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FI.	Customers should conduct due diligence before selecting a service provider, especially in terms of governance, risk and compliance management mechanisms. Customers should develop a list of reputable service providers, and be able to identify whether there are any viable alternatives to the preferred service provider. HUAWEI CLOUD provides online version of HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence by FIs. Customers' 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 ISO27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. Technical ability: HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, HUAWEI CLOUD has created a new 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. 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. 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. Corporate culture and service policies suitable for FIs: HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, 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.
5.4	System Development Life Cycle and Security-By-Design	FIs should establish a framework to manage its system development life cycle (SDLC). The framework should clearly define the processes, procedures and controls in each phase of the life cycle, such as initiation/planning, requirements analysis, design, implementation, testing and acceptance.	Customers should establish a framework to manage its system development life cycle (SDLC) according to the requirements. HUAWEI CLOUD has pursued the new DevOps process, which features rapid and continuous iteration capabilities, and integrated the HUAWEI security development lifecycle (SDL). In addition, gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD hierarchically manages the development environment and implements protection measures

			such as physical isolation, logical isolation, access control, and data transmission channel approval and audit.
5.5	System Requirements Analysis	FIs should identify, define and document the functional requirements for the IT system. In addition to functional requirements, key requirements such as system performance, resilience and security controls should also be established and documented.	Customers should identify, define and document the functional requirements for the IT system, including requirements of system performance, resilience and security controls. HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. Currently, 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.
5.7	System Testing and Acceptance	A methodology for system testing should be	Customers should perform system testing and fixed on a

		established. The scope of testing should cover business logic, system function, security controls and system performance under various load and stress conditions. A test plan should be established and approved before testing.	regular basis for critical businesses and analyze the results. In addition, HUAWEI CLOUD manages vulnerabilities based on its vulnerability management system to ensure that vulnerabilities on self-developed and third-party infrastructure, platforms, application layers, cloud services, and O&M tools are detected and fixed within the time specified in SLA. This reduces risks caused by malicious exploitation of vulnerabilities and adverse impacts on FIs businesses. For vulnerabilities that involve the cloud platform and FIs businesses, HUAWEI CLOUD will push the vulnerability mitigation and recovery suggestions and solutions to end users and FIs in a timely manner after making sure that no high attack risks will be caused by proactive disclosure. HUAWEI CLOUD will face the challenges brought by the security vulnerabilities together with FIs.
5.8	Quality Management	Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI’s policies, procedures and standards.	Customers should perform quality assurance according to the requirements. HUAWEI CLOUD has developed a complete project management approach and is CCM5/CMMI, ISO 9001:2000 and PMI framework based practices which have enabled successful project implementations over the world by qualified project and project management professionals.

6.4 Software Application Development and Management

Chapter 6 of the *Technology Risk Management Guideline 2021* requires FIs to ensure a secure software application development and management. Requirements cover Secure Coding, Source Code Review and Application Security Testing, Agile Software Development, DevSecOps Management, Application Programming Interface Development and Management of End User Computing and Applications. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.1	Secure Coding, Source Code Review and Application Security Testing	To minimize the bugs and vulnerabilities in its software, the FI should adopt standards on secure coding, source code review and application security testing. The secure coding and source code review standards should cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling.	Customers should establish a mechanism for source code security management. To meet customer compliance requirements, HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Source codes are reviewed and approved by the change manager prior to compilation. Developers cannot approve and compile the codes. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding. All cloud services pass multiple security tests before release. The test environment is isolated from the production environment and avoids production data or sensitized production data for testing, which needs to be cleaned up after use.
6.2	Agile Software Development	When adopting Agile software development methods, the FI should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process.	Customers should establish a mechanism for agile software development methods. HUAWEI CLOUD has developed a complete set of software development and privacy activities guidelines. The objectives of this guidelines is to guide and standardize the integration of

			security activities into the R&D process. It provides specific definitions and activity guidelines for product security and privacy requirements. It requires the security planning and security requirement analysis to be integrated in the early planning phase to ensure efficient development of safe and reliable cloud services. During the design phase, privacy risk assessment and security and privacy design will be performed. HUAWEI CLOUD also requires cloud service product team members to take the initiative to learn the basics of security and privacy by taking training courses.
6.3	DevSecOps Management	FIs should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.	Customers should establish a mechanism for DevSecOps management. Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM) to comply the requirement of SoD.
6.4	Application Programming Interface Development	Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.	Customers should adopt strong encryption standards and key management controls to secure transmission of sensitive data through APIs. HUAWEI CLOUD use secure encryption channels (such as HTTPS) during information transmission, and use secure encryption algorithms for stored static data to ensure data confidentiality in different states. Control mechanisms such as digital signatures and timestamps are used to prevent tampering during data transmission, ensure information integrity, and prevent replay attacks. Logs are recorded for operations in application services to support audit. Identity authentication, transmission protection, and

			border protection for interfaces are performed to ensure API application security.

6.5 IT Resilience

Chapter 8 of the *Technology Risk Management Guideline 2021* requires FIs to ensure the availability of their systems and implement and test disaster recovery plans to minimize system and business disruption due to serious incidents. Requirements cover System Availability, System Recoverability, Testing of Disaster Recovery Plan, System Backup and Recovery and Data Centre Resilience. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
8.1	System Availability	IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs. Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability.	Customers can rely on HUAWEI CLOUD data center cluster multi region (Region) and multi-availability 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.
8.2	System Recoverability	The FI’s disaster recovery plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of	HUAWEI CLOUD has various policies and procedures for business continuity management and disaster recovery. Business continuity plans are established and

		relevant personnel in the recovery process. The disaster recovery plan should be reviewed at least annually and updated when there are material changes to business operations, information assets or environmental factors.	reviewed by the business continuity management team annually, and the plans are updated according to results of the review. The business continuity management team performs business impact analysis and risk assessment every year, including identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service level and time needed to resume service. Threats that may lead to disruptions to Huawei Cloud's business and resources are identified and documented in the reports, and corresponding strategies are designed for different service disruption scenarios of Huawei Cloud's products. Results of the business impact analysis and risk assessment are documented in the risk evaluation report. Huawei Cloud conducts a business continuity drill test at least annually in accordance with the plan for all in-scoped products. The results of the business continuity drill test are documented and reviewed.
8.3	Testing of Disaster Recovery Plan	The FI should test the recovery dependencies between systems. Bilateral or multilateral recovery testing should be conducted where networks and systems are linked to specific service providers and vendors. The FI should involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly. The FI should also participate in disaster recovery tests that are conducted by its service provider(s), including those systems which are located offshore.	Customers should establish disaster recovery plans for their key systems, consider whether it involves the collaboration of outsourced suppliers, and regularly test the plans. HUAWEI CLOUD will cooperate actively if it is needed to assist in the implementation of customer disaster recovery plans. Simultaneously, HUAWEI CLOUD has developed its own business continuity plan, in addition to providing features such as improved infrastructure availability, redundant data backup, and disaster preparedness in available areas. The program focuses on major

			disasters such as earthquakes or public health crises to keep cloud services running and secure the customer business and data. Huawei will notify in advance if customer participation is required during the disaster testing of HUAWEI CLOUD.
8.4	System Backup and Recovery	The FI should establish a system and data backup strategy and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted. To ensure data availability is aligned with the FI's business requirements, the FI should institute a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data.	Customers should develop their business continuity mechanisms to back up critical data. Customers can back up data through HUAWEI CLOUD'S data backup archiving service to ensure that data is not lost in the event of a disaster. Additionally, customers can rely on HUAWEI CLOUD's data center cluster multi-region (Region) and multi availability 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 N1 deployment sizing in HUAWEI CLOUD has procedures in place to guide personnel in the administration of the backup process.
8.5	Data Centre Resilience	The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centers (DCs) to identify potential vulnerabilities and weaknesses, and the	Customers should assess the risks of threats and vulnerabilities according to the various possible situations of threats, considering factors such as the building structure of

		protection that should be established to safeguard the DCs against physical and environmental threats.	data centers, the surrounding environment, the infrastructure of data centers, daily security processes, key systems, and physical and logical access control. When financial institutions select a data center provider, they should obtain and evaluate their data center threat and vulnerability risk assessment (TVRA) reports and ensure that the TVRA reports are up-to-date and that the data center provider is committed to addressing any significant vulnerabilities identified. 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 assessments 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 and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and

			resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers.

6.6 Access Control

Chapter 9 of the *Technology Risk Management Guidelines 2021* requires FIs to take appropriate control measures. Requirements cover User Access Management, Privileged Access Management, and Remote Access Management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.1	User Access Management	Employees of vendors or service providers, who are given authorized access to the FI's critical systems and other computer resources, pose similar risks as the FI's internal staff. The FI should subject these external employees to close supervision, monitoring and access restrictions similar to those expected of its own staff.	Customers should establish a mechanism for authentication and access control management of the information system, and restrict and supervise the behavior of the access system. Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**, including support for password authentication, IAM also supports multi factor authentication as an option. 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. In addition, Huawei'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. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure 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.
9.2	Privileged Access Management	FIs should closely monitor employees with high system access rights, and record and review all their system activities.	Customers should establish a mechanism for management of privileged accounts and to closely monitor their usage. To meet customer compliance requirements, administrators of HUAWEI CLOUD-related systems must first pass two-factor authentication before they can access the management plane through a springboard. All operations are logged and sent to the centralized log audit system in time. The audit system has a strong data retention and query capability to ensure that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI

			CLOUD also has a dedicated internal audit department which will regularly audit the activities of the O&M process.
9.3	Remote Access Management	The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards.	Customers should establish mechanisms for remote access management. In addition to managing the identity and permissions of remote access personnel through Identity and Access Management (IAM), HUAWEI CLOUD also provides encrypted transmission methods for customers to choose from, such as VPN and HTTPS. Additionally, HUAWEI CLOUD only has remote access to its internal systems through the HUAWEI CLOUD unified management access gateway and SVN authority. Moreover, strong log auditing is supported on the access gateway to ensure that the operation and maintenance personnel can locate their actions on the target host.

6.7 Data and Infrastructure Security

Chapter 11 of the *Technology Risk Management Guidelines* 2021 requires FIs to ensure the security of their data centers. Requirements cover Data Security, Network Security, System Security and Virtualization Security. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
11.1	Data Security	The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorized access, modification, copying, or transmission of its confidential data.	Customers should identify and classify their important data so that appropriate controls can be taken to secure the data. Regarding data isolation, HUAWEI CLOUD recommends that data be distinguished and isolated at the beginning of the data life cycle by first running a classification and risk analysis on the customer's data. Based on the risk analysis results, clarify the storage location, storage services

			and security measures to protect data. To meet compliance requirements, HUAWEI CLOUD also provides customers with a range of data storage services that follow advanced industry standards for data security lifecycle management using excellent technologies, practices, and processes in authentication, rights management, access control, data isolation, transmission security, storage security, data deletion, and physical destruction. It also ensures that tenant privacy, ownership and control over their data are not infringed upon, providing users with the most effective data protection. For more details, please refer to the *White Paper for HUAWEI CLOUD Data Security*.
11.2	Network Security	To minimize the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets. The FI should install network security devices such as firewalls to secure the network between the FI and the internet, as well as connections with third parties. Network intrusion prevention systems should be deployed in the FI’s network to detect and block malicious network traffic.	HUAWEI CLOUD will immediately analyze and update rules for common CVE vulnerabilities and provide quick and professional CVE vulnerability scanning. Customers can deploy Web Application Firewall (WAF) to detect and protect website service traffic from multiple dimensions. HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the

			public-facing network perimeter, trust boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities. In addition, firewall devices are configured to restrict access to Huawei's production networks. The configurations of firewall policies are configured on machines. A monthly review is performed to ensure firewall rules are configured based on standards. Any changes of firewall rules due to deviations are tracked and remediated. HUAWEI CLOUD restricts the access to high-risk ports and use of high-risk protocols by configuring the firewall policies.
11.3	System Security	The security standards for the FI's hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimize their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.	Customers need to formulate security configuration baselines for every system and periodically check the baselines. Customers need to assess the risks and develop mitigation measures where the configuration is not compliant with security configuration baselines. HUAWEI CLOUD provides Host Security Service (HSS) for customers to identify unsafe items and prevent security risks. HSS can check host baselines, including checking the system password complexity policies, common weak passwords, risky accounts, and common system and middleware configuration. HUAWEI CLOUD has formulated a security configuration baseline for the virtualization operating system to ensure the security when customers using cloud services.
11.	Virtualization	Strong access controls	Policies and procedures for

4	Security	should be implemented to restrict administrative access to the hypervisor and host operating system as both control the guest operating systems and other components in the virtual environment.	logical security are formally established and documented. User accounts belonging to Huawei employees and contractors are approved, added, modified, or disabled in a timely manner and are reviewed on a periodic basis. Huawei has established a set of requirements which consists of the hierarchical authentication system to its internal IT environment, system platform, middleware, network devices and application systems, and related technical requirements. All the access is followed and granted based on the least privileges concept. Bastion host provides a two-factor authentication ("2FA") feature based on password and mailbox verification code to authenticate the identity of users. Users must be authenticated through two factor authentication based on registered devices and their accounts and passwords to access HUAWEI CLOUD office subnet via the Internet. HUAWEI CLOUD employees can perform logical access management in CloudScope which covers various supporting tools such as CloudMNet System, CBC Account Center, bastion host, FUXI and SVN. The supporting tools cover operation systems of all products within the scope of this report, including but not limited to the supporting tools of virtual servers and infrastructure devices. The access authorizations in the supporting tools are enforced at all relevant layers based on the least privileges. Access above the least privileges requires appropriate approvals from the designated approvers.

7 How HUAWEI CLOUD Can Help Customers to Meet the Requirements in MAS Notice on Cyber Hygiene

On August 6, 2019 and November 5, 2019, the MAS issued 11 Notices on *Cyber Hygiene* for different FIs, providing practical guidance for Singapore FIs on compliance with relevant acts. Notice on Cyber Hygiene covers requirements, such as Administrative Accounts, Security Patches, Security Standards, Network Perimeter Defense, Malware Protection and Multi-Factor Authentication.

The following summarizes the requirements for cloud service providers in the Notice on Cyber Hygiene and explains how HUAWEI CLOUD is assisting customers to meet these requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.1	Administrative Accounts	A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account.	Customers should establish a mechanism for management of privileged accounts and to closely monitor their usage. Customers can manage account privileges more effectively through HUAWEI CLOUD's IAM services and PAM functions. Customers can also use the cloud trace service (CTS) as a supplement to provide operational records of cloud service resources for users to query, and for audit. HUAWEI CLOUD implements role-based access control for operations personnel by restricting personnel with different responsibilities in different positions to perform specific operations on authorized

			operational objectives, and granting privileges or contingency accounts only when required by employees' responsibilities. Applications for all privileged or emergency accounts are subject to multiple levels of review and approval. HUAWEI CLOUD will only log in to the customer's console or resource instance to assist the customer in maintenance after it has been authorized by the customer (i.e. providing account/password).
4.2	Security Patches	(a) A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability. (b) Where no security patch is available to address a vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such a vulnerability to such a system.	Customers should establish the vulnerability management process and develop compensation measures for vulnerabilities that cannot be fixed by patches. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools (regardless of whether they are found in Huawei or third party technologies) are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation, and its impact to our customers' services. To protect end users and tenants, HUAWEI CLOUD upholds the principle of responsible disclosure. It ensures no undue risks for potential exploitation and attacks will result from the disclosure of any vulnerability, HUAWEI CLOUD continues to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and tenants vulnerability mitigation solutions, standing shoulder to shoulder with our customers to

			tackle security challenges caused by vulnerabilities.
4.3	Security Standards	(a) A relevant entity must ensure that there is a written set of security standards for every system. (b) Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards. (c) Where the system is unable to conform to the set of security standards, the relevant entity must ensure that controls are instituted to reduce any risk posed by such non-conformity.	Customers need to develop security configuration baselines for all systems and periodically check the baselines. Risk assessment must be performed to develop compensation measures for non-compliance with the security configuration baseline. Customer can check host baselines through HUAWEI CLOUD **Host Security Service (HSS)**[2]. It can check system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks.
4.4	Network Perimeter Defense	A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic.	Customers need to divide their networks into security zones and strictly control access between different security zones. To complement our customers' requirements, in the initial phase, HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the public-facing network perimeter, trust

			boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities.
4.5	Malware protection	A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented.	Customers need to deploy antivirus software on all systems. In addition, in order to ensure the safe and stable operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness.
4.6	Multi-factor Authentication	A relevant entity must ensure that multi-factor authentication is implemented for the following: (a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and (b) all accounts on any system used by the relevant entity to access customer information through the internet. This requirement may not be met if the relevant entity identifies all risks posed by its non-compliance with this	Customers need to ensure that multi-factor authentication is implemented for all administrative accounts of critical systems and all accounts that can access end customer information. In exceptional circumstances, customers shall identify and access all risks posed by its non-compliance with this requirement, and the senior management or the committee should accept the risks or implement controls to reduce the risks. Customers can manage user accounts using cloud resources through HUAWEI CLOUD **IAM**, including support for password authentication, IAM

		requirement between 6 August 2020 and 5 February 2021, and the senior management or the committee of the relevant entity accepts the risks or implements controls to reduce the risks.	also supports multifactor authentication as an option. To meet the requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. In addition, administrators of HUAWEI CLOUD-related systems must first pass two-factor authentication before they can access the management plane through a springboard. All operations are logged and sent to the centralized log audit system in time.

8 How HUAWEI CLOUD Can Help Customers to Meet the Requirements in ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers

The ABS *Guidelines on Control Objectives and Procedures for Outsourced Service Providers* provides control objectives and process guidelines for outsourcing service providers of FIs operating in Singapore. The guideline sets out minimum/baseline control requirements that the outsourcing service providers of FIs must adhere to, including audits and inspections, entity level controls, general IT controls, and service controls. In addition to these control requirements, the outsourcing service provider is required to provide the relevant third-party audit report (OSPAR).

The following will summarize the control requirements related to cloud service providers in *Guidelines on Control Objectives and Procedures for Outsourced Service Providers* and explain how HUAWEI CLOUD will help them meet these control requirements.

8.1 Audits and Inspections

The guideline clearly requires that outsourcing service providers providing services to FIs need to engage external auditors regularly for auditing and provide OSPAR audit reports in accordance with the requirements of said guideline. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
I	Engagement of external auditor	The OSP should engage a qualified auditor to perform audits in accordance with these Guidelines on the services rendered to the FIs. In the event that an OSP decides to change the external auditor or decides to appoint a different external auditor	HUAWEI CLOUD has obtained a number of internationally authoritative security and compliance certifications. HUAWEI CLOUD employs professional third-party auditors each year to audit its cloud computing products and services. In order to build up the
II	Criteria for qualification external auditor		

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		for validation of remediation activities, the OSP must ensure that there is a proper hand-over from the outgoing auditor to the incoming auditor to ensure that the interests of the FIs remain protected. The appointed external auditor should demonstrate a sound understanding of outsourcing risks pertinent to the banking industry as well as fulfill the following criteria: 1. The audit firm must have audited at least 2 commercial banks operating in Singapore in the last 5 years; and 2. The engagement partner, who signs off the Audit Report, must have audited at least 2 commercial banks operating in Singapore in the last 5 years.	confidence of Singapore's FIs in HUAWEI CLOUD, HUAWEI CLOUD will use this as a guide when selecting an audit institution to ensure that the selected audit institution has extensive audit experience in the Singapore banking industry and can meet the qualifications required by the guide for external auditors. If the audit institution is replaced, HUAWEI CLOUD will follow internal processes to ensure that the work is fully transitioned to the new audit institution.
III	Frequency of audit	The audit should be performed once every 12 months. To be useful to FIs relying on the report, the samples selected for testing the operating effectiveness of controls should cover the entire period since the previous audit, with a minimum testing period of 6 months. If the period is less than 6 months, the reasons for the shorter period should be provided in the report. The appointed external auditor should issue the audit report in the format stated in the Outsourced Service Provider Audit Report ("OSPAR") template. The OSP must furnish a copy of its audit report to its FI clients.	HUAWEI CLOUD employs professional third-party auditors to audit cloud computing products and services provided by HUAWEI CLOUD every year, and publishes audit reports in accordance with the format specified in the OSPAR template. After the report is formed, HUAWEI CLOUD will issue copies of audit reports to customers in the financial industry according to internal processes.
IV	Audit report		
V	Reporting and	If the auditor finds	HUAWEI CLOUD will provide

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	handling of control failure /qualification of control objectives	insufficient design and/or operational effectiveness of the control activities associated with the control objective, the auditor should assess the potential impact of the failure on the services of the institution. The relevant audit standards provide for the identification procedures for control objectives, which the auditors should follow. Outsourcing service providers should inform financial institutions of major issues and concerns and remedial plans no later than the release date of the OSPAR. However, if the problem may lead to the failure or interruption of long-term services in outsourcing arrangements, or violate the security and confidentiality of customer information of financial institutions, the outsourcing service provider should notify the financial institutions immediately after the problem occurs. Outsourcing service providers should develop remediation plans to address audit findings. If the problem takes longer to correct, the outsourcing service provider should identify short-term measures to mitigate the risk. Remedies should be verified by the auditor or other competent independent parties.	audit samples to verify the effectiveness of HUAWEI CLOUD security and compliance control measures, such as security system management documents, operating records and system logs. This is in accordance with the requirements of external audit institutions. If special circumstances lead to insufficient time to cover audit samples, HUAWEI CLOUD will cooperate with the audit institutions to indicate the reasons in the audit report. In view of all the problems found in the audit process, HUAWEI CLOUD will assess the potential impact of these problems on financial industry customers with the assistance of audit institutions and according to the risk assessment mechanism. If after evaluation, problems that may seriously affect the availability, integrity and confidentiality of customer business/data are identified, HUAWEI CLOUD will classify such problems as security incidents, and promptly notify the affected customer groups according to the established customer notification process. This includes the description of the problem, the impact of the problem, and the next remedial plan. At the same time, HUAWEI CLOUD will rectify the problem according to the internal security incident management process, and the audit institutions will reassess the problem after the rectification is completed.
VI	Rights of FIs and MAS	Monetary Authority of Singapore (MAS) and financial institutions have the right to audit outsourced service providers and	Customers should establish formal audit procedures and regularly audit their outsourcing suppliers. HUAWEI CLOUD will actively

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		subcontractors of outsourced service providers.	cooperate with MAS and FIs to audit HUAWEI CLOUD and its suppliers.

8.2 Entity Level Controls

The control requirement at the first part of the *Guidelines on Control Objectives and Procedures for Outsourced Service Providers* is entity-level control, which pertains to enterprise internal controls to ensure that the outsourcing service provider executes management instructions related to the entire entity. Entity-level controls mainly consist of control environment, risk assessment, information and communication, monitoring, information security policies, HR policies and practices, and practices related to sub-contracting. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
I.(a)	Control environment	The control environment sets the priority and culture for the OSP, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure, and therefore implements it top-to-bottom through its entire governance structure.	In order to continuously improve employees' security awareness, protect customer interests, and boost product and service reputation, Huawei advocates company-wide for a mindset and practice wherein "everyone understands security", cultivating a security culture that is present 24/7, as well as dynamic and competitive throughout the company. The impact of such a culture runs through talent recruitment, new-hire orientation, initial and ongoing training, internal transfer, and internal re-training, all the way up to employment termination. Huawei prioritizes cybersecurity as one of the company's key strategies, and therefore implements it top-to-bottom through its entire governance structure. From an organizational structure perspective, the GSPC functions as the highest

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			cybersecurity management organizational unit, making decisions on and issuing approvals of the company's overall cybersecurity strategy. The GSPO and its office are responsible for formulating and executing Huawei's end-to-end cybersecurity framework. The GSPO reports directly to the company's CEO.
I.(b)	Risk assessment	The risk assessment process of the outsourced service provider may have an impact on the services provided to financial institutions. The following is a list of risk assessment factors: • Changes in Operating Environment • New personnel • New or revamped information systems • Rapid growth • New technology • New business models, products or activities • Corporate restructurings • Expanded foreign operations • Environmental Scanning	HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts an annual risk assessment and increases the number of risk assessments for major changes in information systems, a significant change in the company's business, or a significant change in laws, regulations or standards.
I. (c)	Information and communicatio n	The internal control information and communication section of the outsourcing service provider should include how the information system must document the procedures for initiating, authorizing, recording, processing and reporting on transactions of financial institutions, how the outsourcing service provider communicates its roles and responsibilities, and how they communicate important matters related to the services provided to the financial institution.	Customers can get information about cloud services provided by Huawei through the HUAWEI CLOUD official website. HUAWEI CLOUD provides a unified hotline, email address, and work order system to handle service requests from FIs. HUAWEI CLOUD will also establish links with relevant regulatory bodies to facilitate necessary communication.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
I. (d)	Monitoring	The OSP may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, either by ongoing activities, periodic evaluations, or combinations of the two. OSPs should have processes in place to bring significant issues and concerns identified through such evaluation to the OSPs' senior management and additionally, if impacting the services provided, e.g. adverse developments, to the FIs. The OSP's monitoring of its sub-contractors' activities that affect the services provided to the FIs is another example of monitoring. This form of monitoring may be accomplished through visiting the sub-contractors' organization, obtaining and reading reports containing detailed description of the sub-contractors' controls, or conducting an independent assessment of whether the controls in place are suitably designed and operating effectively throughout the specified period. Copies of any such reports and findings made on the OSP and/or its sub-contractors, in relation to the outsourcing arrangement, must be provided to the FIs. Results should be discussed as part of ongoing service discussions. Monitoring external communications, such as customer complaints and communications from regulators, would be important and results of such monitoring should be provided to FIs.	Huawei has established a dedicated safety audit team to review compliance with global safety laws and regulations and internal safety requirements. Huawei's internal audit team reports directly to the board of directors and senior managers of the company to ensure that the problems found are solved and ultimately closed. Strict audit activities play a key role in promoting the process and standards of network security and ensuring results are delivered. In addition, HUAWEI CLOUD has established a complete supplier selection and management mechanism, including day-to-day monitoring and supplier performance management, but also regularly conducts risk assessment for suppliers. HUAWEI CLOUD will inform FIs of problems identified in audits and re-evaluate them within the organization, particularly if the problems have a significant impact on the business of the financial institution. HUAWEI CLOUD provides a unified communication interface with the outside world. It is responsible for collecting and handling complaints from customers and issuing announcements to financial customers from regulatory agencies.
I. (e)	Information security policies	Information Security ("IS") policies and procedures are established, documented and reviewed at least every 12	Customers should establish and regularly review formal information security policies and processes.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		months or as and when there are changes. IS policies and procedures should state the person(s) responsible for information security management. These documents are reviewed and approved by management. Specific security controls for systems and networks are defined to protect the confidentiality, integrity and availability of systems and data. Any identified deviations are documented, tracked and remediated. Deviations which impact the services rendered should be communicated to the FIs immediately. An information security awareness training programme should be established. The training programme should be conducted for OSP's staff, subcontractors and vendors who have access to IT resources and systems regularly to refresh their knowledge.	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. In addition, HUAWEI CLOUD focuses on the development of safety awareness among employees and outsourcing personnel, and has developed an applicable safety awareness training program that is applied regularly.
I. (f)	Human resources (HR) policies and practices	FIs expect sub-contractors of OSPs to be managed with the same rigour as the OSPs themselves. Thus, OSP should require and ensure that their sub-contractors adhere to the requirements of these Guidelines.	Consistent with that of the entire company, the HR management framework for HUAWEI CLOUD security personnel has been long established on the basis of applicable laws. Cloud security requires HR to ensure that our staff's backgrounds and qualifications meet the requirements of HUAWEI CLOUD services. HUAWEI CLOUD employees must

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			consistently demonstrate the required knowledge, skills, and experience. The behavior of each HUAWEI CLOUD employee must comply with applicable laws, policies, and processes, as well as the Huawei Business Conduct Guidelines (BCG). HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers. This program includes: On-boarding security review, On-the-job security training and enablement, On-boarding qualifications management, Off-boarding security review.
I.(g)	Practices related to subcontracting	FIs want subcontractors for outsourced service providers to be as strictly regulated as outsourcing service providers themselves. Therefore, outsourcing service providers should require and ensure that their subcontractors comply with this guide	HUAWEI CLOUD has developed its own mechanism for supplier management as suppliers have raised their security requirements for their own products and internal management. In addition, HUAWEI CLOUD will also conduct regular audits of suppliers as at-risk suppliers will be audited on-site. Moreover, network security agreements are signed with vendors involved in network security, and the quality of service is continuously monitored as vendor performance is evaluated during the service process, and vendors with consistently poor security performance will be downgraded.

8.3 General IT Controls

Part II of the *Guidelines on Control Objectives and Procedures for Outsourced Service Providers* is general IT controls that cover different areas of cyber security, including logical security, physical security, change management, incident management, backup and disaster recovery, network and security management, security incident response, system vulnerability assessments, and technology refresh management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
II.(a)	Logical security	FIs should ensure that logical access to programs, data and operating system software is limited to authorized personnel only in accordance with the on-demand principle. Financial institutions should periodically review application/system passwords in accordance with agreed information security requirements /standards so as to have strict control over the use of accounts with high access rights.	Section "6.6 Access Control "details how HUAWEI CLOUD meets requirements for authentication and access control.
II.(a)	Logical security	Establish processes to securely destroy or delete financial institution data each time the service is terminated in accordance with the agreed retention and destruction policy. This requirement also applies to backup data.	HUAWEI CLOUD strictly follows the data destruction standard and the agreement between the customer to erase stored customer data when a customer deletes data or data is deleted due to expiration of the service. For more information on data deletion, please refer to section 4.8 *Permanent Destruction* in the *White Paper for HUAWEI CLOUD Data Security*.
II.(a)	Logical security	Deploy industry-recognized encryption standards and agree with financial institutions to protect financial institution customer information and other sensitive data in accordance with MAS Technical Risk Management (TRM) guidelines.	HUAWEI CLOUD encapsulates complex data encryption and decryption, and key management logic. At present, cloud hard disk, object storage, image service, relational database and other services all provide data encryption (server-side encryption) function using high-intensity algorithm to encrypt the stored data. 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 ensures data security on the cloud. DEW adopts the layered key management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			mechanism. Specifically, after association configuration on DEW Console or using APIs, customer's master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. 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.
II.(b)	Physical security	Data center/control areas should be physically protected from internal and external threats. These include restricting access to data centers/control areas, installing intrusion alerts at all entrances, tracking audits of access to secure areas, periodic review of access to data centers, managing physical access credentials, and performing threat and vulnerability risk assessments (TVRA). Data centers/control areas should also be resilient to protect IT assets. This includes the installation of a complete environmental control system, and environmental control equipment for inspection, testing and maintenance.	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. For more information, please refer to the physical and environmental safety section of the *White Paper for HUAWEI CLOUD Data Security*.
II.(c)	Change management	FIs should evaluate, approve, test, implement and review changes to applications, system software, and network components in a controlled manner. Establish development,	Customers should establish formal change management procedures and regularly review the implementation of changes, particularly the source code. Customers should ensure that their development, testing, and production environments are isolated from one another, and that the use of different

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		testing, grading, and production environment isolation. UAT data should be anonymous, and if the UAT contains production data, the environment must be controlled at the appropriate production level. Review source code of high-risk systems and applications update to identify security vulnerabilities, code errors, defects, and malicious code before implementing these changes.	environments is controlled strictly. To meet customer compliance requirements, HUAWEI CLOUD has also developed change management procedures to application and infrastructure changes. After the change application is generated, the change manager shall make a change level judgment and submit it to the HUAWEI CLOUD change committee, which shall pass the review before implementing the change as planned. All changes are fully validated prior to application through class production, bad condition testing, gray release, Blue Green Deployment, etc. to ensure that the change committee has a clear understanding of the change action, duration, fallback action of the change failure, and all possible impacts. HUAWEI CLOUD isolates development, testing, and production environments, and strictly controls the flow of unsensitized data into the testing environment; HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding.
II.(d)	Incident management	The problems of system and network operation should be solved in a timely and controllable manner. Ensure that there is a formally documented incident management process that clearly documents the roles and responsibilities of employees involved in the incident management process, including documentation, analysis, repair, and monitoring of issues and events, while documenting the upgrade	Customers should establish formal event management procedures to solve system and network failures in a timely manner. In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and solution agreements and timelines, recording and tracking the information about incidents, analyzing the cause of the incident, identifying the root cause, and preventing the occurrence of the incident from happening again.	have on the customer's business. The contents of the notice include, but are not limited to, descriptions of the incident, causes, impacts, actions taken by HUAWEI CLOUD, and measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues.
II.(e)	Backup and disaster recovery	Perform backup and secure storage; Record, approve, test, and maintain business and information system recovery and continuity plans.	Customers should develop their business continuity mechanisms to back up critical data. Customers can back up data through HUAWEI CLOUD's **data backup archiving service** to ensure that data is not lost in the event of a disaster. Additionally, 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 N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.
II.(f)	Network and security management	System and network control are based on the business needs of customers. Specific security controls for systems and networks should be defined, as well as for security baseline	Customers should establish formal systems and network management procedures. To complement our customers' compliance requirements, Huawei's dual role as a developer and cloud service operator of cloud technology is responsible for its CSP infrastructure and the security of its own

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		standards and various middleware, operating systems, databases, and network devices. Processes should be performed to ensure that anti-virus/anti-malware processes are installed and updated on a regular basis. Patch management processes should be established, security policy/standard deviations should be documented, and controls should be implemented to reduce risk. File integrity checks and deployment of network security controls are needed to protect internal networks through the regular backup and review of network security equipment rules while recording, saving, and monitoring security system events.	services (i.e. IaaS, PaaS and SaaS). HUAWEI CLOUD ensures that development, configuration, deployment, and operation of various cloud technologies is secure. Therefore, in the initial phase, HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. In addition, in order to ensure the safe and stable operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness.
II.(g)	Security incident response	It should ensure that appropriate personnel can be contacted when security incidents occur, and immediate measures should be taken in response to security incidents.	HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices. Incidents will be ranked based on the extent to which security incidents affect the customer's business, and will initiate a customer notification process to notify customers of the incident. After the event is resolved, an event report will be

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			provided to the customer.
II.(h)	System vulnerability assessments	Outsourced service providers continuously monitor emergency security vulnerabilities and conduct periodic vulnerability assessments of IT environments to address common and urgent internal and external security threats. The frequency of vulnerability assessment should be based on the risk assessment of financial institutions and reach consensus with financial institutions. Outsourcing service providers perform penetration testing of Internet-oriented systems at least once every 12 months. Problems identified through vulnerability assessment and penetration testing are repaired and re-validated in a timely manner to ensure that identified gaps have been fully addressed.	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 exposure. Additionally, HUAWEI CLOUD will actively implement quality assurance of cloud product and platform security, and conducts internal and third-party penetration testing and security assessments each year to ensure the HUAWEI CLOUD environment is secure.
II.(i)	Technology refresh management	Implement control measures to ensure that software and hardware components used in production and disaster recovery environments are updated in a timely manner. This includes documenting and reviewing technology update management plans and processes at least every 12 months. In the event of changes, maintain up-to-date inventory of software and hardware components used in production and disaster recovery environments that support financial	Customers can rely on HUAWEI CLOUD 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 N1 deployment sizing in the data center

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		institutions to facilitate the tracking of IT resources, and outsourcing service providers actively managing their IT systems and software to support financial institutions The outsourcing service provider shall inform the financial institution of the system it identifies to be replaced or discontinued; When stopping using IT systems, outsourcing service providers should ensure that financial information security is destroyed/cleared from the system to prevent data leakage; conduct risk assessment of systems approaching the termination of technical support (EOS) date, assess the risks that may arise from continued use, and establish effective risk mitigation control measures where necessary.	while balancing traffic load to other centers, even in the event of a data center failure. In addition to providing high-availability infrastructure, redundant data backup centers, and disaster preparedness in available areas, HUAWEI CLOUD has also developed business continuity plans and disaster recovery plans that are regularly tested to ensure that the emergency plan is in line with the current organizational and IT environment. HUAWEI CLOUD is committed to protecting tenant data from disclosure during and after deletion. When a customer initiates a data deletion operation or if the data needs to be deleted due to the expiration of the service, HUAWEI CLOUD will strictly follow the data destruction standard signed by agreement with the customer to erase the stored customer data. The types of data deletions involved include: memory deletion, data security (soft) deletion, disk data deletion, encrypted data to prevent leakage and physical disk scrap.

8.4 Service Controls

Part III of *Guidelines on Control Objectives and Procedures for Outsourced Service Providers* requires service controls that cover the management of the outsourcing service provider's service to financial institutions, including setting-up of new clients/processes, authorizing and processing transactions, maintaining records, safeguarding assets, service reporting and monitoring. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
III.(a)	Setting-up of new clients/ processes	Develop and monitor the outsourcing service provider contract process. The process of outsourcing service	Customers should establish formal procedures for managing outsourcing contracts. HUAWEI CLOUD cooperates with customers to meet compliance requirements and exercise supervision over cloud service providers. The online

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		providers is established and managed in accordance with the agreements and instructions of financial institutions.	*HUAWEI CLOUD Customer Agreement* defines the security responsibilities of cloud service customers and Huawei, while the *HUAWEI CLOUD Service Level Agreement* stipulates the service level provided by HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be negotiated with customers to meet their requirements. HUAWEI CLOUD will follow the contract process of its customers to some extent and if necessary, HUAWEI CLOUD will actively cooperate with customer inspection and due diligence. At the same time, HUAWEI CLOUD has also developed its own supplier management mechanism as suppliers have raised their security requirements towards their own products and internal management. In addition, HUAWEI CLOUD will also conduct regular audits of suppliers as at-risk suppliers will be audited on-site. Moreover, network security agreements are signed with vendors involved in network security, and the quality of service is continuously monitored as vendor performance is evaluated during the service process, and vendors with consistently poor security performance see reduced cooperation.
III.(b)	Authorizing and processing transactions	Outsourcing service provider services and related processes should be authorized and documented fully, accurately, and timely, subject to internal inspection to reduce the likelihood of errors. Services are processed in stages by independent parties, and therefore have separation of responsibilities from start to finish.	Customers should manage the services of outsourced service providers. To meet customer compliance requirements, HUAWEI CLOUD has developed a complete service management system, and passed the ISO 20000 certification, to ensure that effective IT services meet customer needs.
III.(c)	Maintaining record	The data is classified according to sensitivity, which	To ensure customer security, HUAWEI CLOUD protects data in all stages of its lifecycle, from data creation, data storage,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		determines data protection requirements, access rights and restrictions, and retention and destruction requirements.	data use, data sharing, and data archiving, to data destruction. It facilitates the use by customers through a friendly interface to meet the personalized needs for data security of customers in different industries. For more details, please refer to the *White Paper for HUAWEI CLOUD Data Security*.
III.(d)	Safeguarding assets	Protect physical assets from loss, abuse and unauthorized use.	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. Please refer to physical and environmental safety section of *White Paper for HUAWEI CLOUD Security*.
III.(e)	Service reporting and monitoring	Outsourcing activities are properly managed and monitored.	Customers should manage and monitor outsourcing activities. Customers can monitor the usage and performance of their cloud resources through the HUAWEI CLOUD monitoring service. HUAWEI CLOUD can also report on SLA services according to customer needs.

9 How HUAWEI CLOUD Can Help Customers to Meet the Requirements of ABS Cloud Computing Implementation Guide

In August 2019, ABS released the *ABS Cloud Computing Implementation Guide 2.0*, which provides FIs with best practices and considerations on using cloud services, including recommendations for due diligence of cloud service providers and key controls to be considered when adopting cloud services.

The following summarizes the control requirements related to cloud service providers in *ABS Cloud Computing Implementation Guide 2.0* and details how HUAWEI CLOUD, as a cloud service provider of FIs, can help FIs meet these control requirements.

9.1 Activities Recommended as Part of Due Diligence

Section 3 of *ABS Cloud Computing Implementation Guide 2.0* provides FIs with recommended due diligence and vendor management activities in the use of cloud services, covering pre-engagement of the cloud service providers as well as ongoing risk assessments and oversight. The guidance proposals mainly include governance, assessment of cloud service providers, and contractual considerations. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
1	Governance	Financial institutions should ensure that contractual terms and conditions regarding the roles, relationships, obligations, and responsibilities of all parties are adequately defined in written agreements with cloud service providers. As well as	In line with customer regulation for technology outsourcing, the online *HUAWEI CLOUD Customer Agreement* divides the security responsibilities of cloud service customers and Huawei, while the *HUAWEI CLOUD Service Level Agreement* defines the level of services provided by HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which stipulates that if HUAWEI CLOUD should hire

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		KPI, key activities, inputs and outputs of cloud services purchased and accountability in case of breach of agreement. Financial institutions should conduct due diligence to understand the services they are using and the responsibilities of financial institutions and cloud service providers. Cloud service providers should be able to demonstrate that they implement and maintain a strong risk management and governance framework that effectively manages cloud service arrangements, including any subcontracting arrangements.	subcontractors, HUAWEI CLOUD shall notify customers and be responsible for the subcontracting services according to customer requirements. HUAWEI CLOUD clearly defines a model for sharing security responsibilities with customers. Customers can find specifics in the *HUAWEI CLOUD Security White Paper* on the HUAWEI CLOUD official website. HUAWEI CLOUD has developed a complete information security risk management framework. It also carries out strict security management for outsourcers, and regularly audits and evaluates its suppliers. HUAWEI CLOUD has obtained the ISO 27001 certification, and employs external professionals for SOC2 certification every year. HUAWEI CLOUD has introduced detailed daily practices for safe operation and maintenance in the *HUAWEI CLOUD Security White Paper*.
2	Assessment of the cloud service providers	FIs are required to conduct due diligence on cloud service providers, including: financials, corporate governance and entity control, data center geographic location, physical security risk assessment, due diligence process, and subcontracting.	**Financial situation:** Huawei publishes its annual report every year. The report covers HUAWEI CLOUD's revenue and is open to the public. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. According to the *Q1 China Public Cloud Service Market Tracking Report 2019* released by IDC, a global authoritative consulting agency, Huawei's cloud revenue has grown by more than 300% in terms of overall market share of IaaS and PaaS, and Huawei's cloud PaaS market share grew by nearly 700%, ranking first in the growth rate of top 5 providers and in China's public cloud service providers.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Corporate governance and entity control: HUAWEI CLOUD upholds that it must put the company's responsibility for network and business security and protection above the company's commercial interests. Cyber security is one of the facets Huawei aims to develop and strategize. HUAWEI CLOUD continues safety awareness training for employees during their employment. There is a special information security awareness training program for employees. This training includes but is not limited to, on-the-spot speeches and online video courses. **Data Center Location**: Customers can purchase cloud services using their own choice of data center. 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 investigating security incidents or investigating violations of contractual requirements. **Physical security risk assessment:** HUAWEI CLOUD regularly conducts risk assessment in data centers around the world, generates assessment reports, and develops detailed risk management plans for risks identified during the assessment process. **Due diligence process**: HUAWEI CLOUD will arrange special personnel to cooperate with FIs to assist them in inspection and due diligence. HUAWEI CLOUD has also taken the initiative to engage professional third-party auditors for cloud computing products and services provided by HUAWEI CLOUD to assure customers that the

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			requirements in their due diligence inspection are met by HUAWEI CLOUD. Audit reports will also be issued in the format specified in the Outsourced Service Provider Audit Report (OSPAR) template. Once the report is finalized, HUAWEI CLOUD will issue a copy of its audit report to financial industry customers in accordance with internal processes. **Subcontracting**: Huawei Group has complete supplier and outsourcing management standards. HUAWEI CLOUD also follows the Huawei group management regulations for outsourcing.
3	Contractual considerations	FIs should ensure that contract agreements with cloud service providers include provisions on data confidentiality and control, data transmission and data location, auditing and inspection, business continuity management, service level agreements, data retention, termination of default, and exit plans.	To complement the customer's oversight of cloud service providers, HUAWEI CLOUD's online *HUAWEI Cloud User Agreement* defines the security responsibilities of cloud service customers and Huawei, and the *HUAWEI CLOUD Service Level Agreement* defines the level of services provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed an offline contract template, which can be negotiated based on customer requirements.

9.2 Key Controls Recommended When Entering into a Cloud Outsourcing Arrangements

Section 4 of *ABS Cloud Computing Implementation Guide 2.0* specifies the minimum/baseline control that financial institutions should implement when entering cloud outsourcing arrangements, as well as additional control measures for important and key tasks. The guidelines categorize the areas of control according to the stage of cloud services usage: govern the cloud, design and secure the cloud, and run the cloud. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Govern the Cloud (setup and on-going management)			
1	Organizational considerations for the management of CSPs	FIs should conduct strong and timely oversight of risks associated with cloud outsourcing arrangements, including due diligence on cloud service providers, monitoring SLA performance, and monitoring of risks associated with security incidents. There should be appropriate channels of communication between the business and operations departments of financial institutions and cloud service providers.	To satisfy the customer's requirements for supervision of cloud outsourcing arrangements, HUAWEI CLOUD provides a unified hotline, mailbox address, and work order system to handle customer service requests. If customers need to conduct due diligence on HUAWEI CLOUD, HUAWEI CLOUD will be responsible for arranging personnel for communication, as HUAWEI CLOUD will provide cloud monitoring services to customers to monitor the use and performance of their own cloud resources, and can provide customized service reports according to customer needs and SLA. This service may incur some cost.
3	Billing models	FIs should manage their cloud resources and costs. Ensure that key service monitoring based on service level protocol is in place, and establish a protocol with CSP to prevent cessation of services based on quotas being exceeded.	To meet customers' requirements for service quotas, HUAWEI CLOUD will compile detailed price lists for service consumption, and tenants can account for their own consumption. Customers can monitor account consumption in the HUAWEI CLOUD management console. Consumption exceeding quotas will result in reminders to tenants, to help them manage their quota and prevent service interruptions due to the depletion of available quota. In addition,the **Cloud Eye Service** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			personalized report views to help accurately grasp the status of business resources.
Design and Secure the Cloud (pre-implementation)			
1	Cloud architecture reference solutions and practices	FIs should create a cloud product service catalogue that meets the internal policies and regulatory requirements of financial institutions, and design and implement the optimized cloud services.	HUAWEI CLOUD provides financial customers with specialized financial industry solutions to help them quickly deploy their cloud services.
2	Virtualization, containerization and DevOps	Manage the confidentiality and integrity risks associated with data co-mingling or shared tenancy environments. • In the event of a software or hardware failure, ensure that information assets remain secure or are securely removed • Define a standard set of tools and processes to manage containers, images and release management	Customers should consider establishing standardized containers and images for release management. Additionally, HUAWEI CLOUD provides an image service to support **Elastic Cloud Service (ECS)**. Customers can choose standard or privatized images provided by the HUAWEI CLOUD official website. Version and release management can be easily carried out through the console. In addition, HUAWEI CLOUD guarantees the security of customer information in multi-tenant scenarios using network isolation, data isolation, external threat defense, identity authentication, access control, and more. For more details, please refer to the *HUAWEI CLOUD Security White Paper*. Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3	Resiliency in cloud architecture	FIs need to carefully consider and plan their cloud adoption to ensure that the resiliency and availability of the cloud services commensurate with their needs.	Customers rely on the multi-region and multi-available area (AZ) architecture of HUAWEI CLOUD data center cluster to achieve the flexibility and availability 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 N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.
4	Network architectures	FIs should implement measures to protect the cloud environment and internal environment to reduce the risk of threat proliferation and ensure that cloud-based businesses are protected from network attacks. Financial institutions should ensure that access to the cloud environment is granted as needed.	HUAWEI CLOUD helps customers build a network security protection system to secure their cloud services. Customers at the Internet border can detect and clean abnormal traffic and traffic attacks by doing the following: deploying **Anti-DDoS services**; partitioning and isolating key network partitions through Virtual Private Cloud (VPC) and deployment of a **Web Application Firewall (WAF)** to deal with web attacks to protect web application services and systems deployed in the DMZ area that are oriented to the external network. In order to ensure that the tenant business does not affect the management operation and that the equipment, resources and traffic will not be separated from effective supervision, HUAWEI CLOUD divides the communication plane of its network into a tenant data plane, business control plane, platform operation and maintenance plane, BMC (Baseboard Management Controller) management plane, and number based on different business functions, different security risk levels, and different permissions, in accordance to the storage plane, to ensure that the network traffic related to different services

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			is reasonably and safely diverted so as to facilitate the separation of responsibilities.
5	Cryptographic key management	FIs should manage encrypted materials so that the confidentiality and integrity of financial institutions ' data will not be compromised, including regular key rotation, detailed policies, and procedures to manage the life cycle of encrypted materials and their backup.	HUAWEI CLOUD provides Data Encryption Workshop (DEW) for customers. The key management function in DEW can centralize key management throughout the life cycle. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, customer's master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. 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.
6	Encryption	FIs should ensure that only authorized parties have access to data in transit and static. FIs should ensure the confidentiality and/or integrity of the data and provide authentication of the source and the non-repudiation of the message.	Customers should establish data management mechanism to ensure data confidentiality and integrity. Customers can encrypt data through HUAWEI CLOUD's data storage and encryption service. HUAWEI CLOUD encapsulates complex data encryption and decryption, and key management logic, which makes the operation of customer's data encryption easy. At present, cloud hard disk, object storage, mirror service and relational database, and other services provide data encryption (service-side encryption) function using high-intensity algorithms to encrypt stored data. The encryption function of the server integrates the key management function (DEW) of Huawei's cloud data encryption service. The HSM used in this function has passed strict international security certification and can prevent intrusion and tampering. Even Huawei's operation and maintenance personnel cannot steal the root key of customers. For data in transmission, when

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. 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.
8	Authentication & user access management	FIs should consider the whole life cycle of user access management to ensure that users can only access the information assets they need to perform their duties. This ensures the confidentiality and integrity of data, and the separation of responsibilities of sensitive roles.	Customers should develop a mechanism for authentication and access management to control employee access to the assets. HUAWEI CLOUD's unified Identity and Access Management (IAM) provides cloud resource access control for customers. With IAM, the customer administrator can manage user accounts and control the accessible to these user accounts. When multi-user cooperative operation resources exist in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and ensure the security of user accounts by setting a login authentication strategy, password strategy and access control list. Through the above measures, we can effectively control privileges and provide emergency accounts. Customers can also use the cloud trace service (CTS) as a supplement to provide operational records of cloud service resources for users to query, and for audit. At the same time, when HUAWEI CLOUD operators access the HUAWEI CLOUD management network for centralized management of the system, they need to use the only identifiable employee identity account. User accounts are equipped with strong password

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			security policies, and passwords are changed regularly to prevent brute-force cracking. Two-factor authentication (2FA) is also used to authenticate cloud personnel, such as with a USB key, smart card and so on. Employee accounts are also used to log on to the VPN and access gateway to further contain user logins for auditing.
9	Privileged user access management (PUAM)	FIs should properly manage access to privileged users and ensure that third-party service providers can access their information assets only through authorized exceptions.	Customers can manage account privileges more effectively through HUAWEI CLOUD's IAM services and PAM functions. To meet compliance requirements, HUAWEI CLOUD implements role-based access control for operations personnel by restricting personnel with different responsibilities in different positions to perform specific operations on authorized operational objectives, and granting privileges or contingency accounts only when required by employees' responsibilities. Applications for all privileged or emergency accounts are subject to multiple levels of review and approval. HUAWEI CLOUD will only log in to the customer's console or resource instance to assist the customer in maintenance after it has been authorized by the customer (i.e. providing account/password).
10	Administrative remote access	FIs should manage various levels of remote access to platforms and systems in their cloud environments. Cloud service providers should also manage remote access to their own systems.	Customers should establish mechanisms for remote access management. In addition to managing the identity and permissions of remote access personnel through Identity and Access Management (IAM), HUAWEI CLOUD also provides encrypted transmission methods for customers to choose from, such as VPN and HTTPS. Additionally, HUAWEI CLOUD only has remote access to its internal systems through the HUAWEI CLOUD unified management access gateway and SVN authority. Moreover, strong log auditing is supported on the access gateway to ensure that the operation and maintenance personnel can locate their actions on the

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			target host.
11	Data loss prevention	FIs should develop comprehensive data loss prevention policies to secure data transferred to and stored in the cloud from unauthorized or unintentional disclosure, while also monitoring and controlling approved and unapproved data transfers and access to cloud services.	Customers should establish formal mechanisms for data protection. To meet compliance requirements, HUAWEI CLOUD provides customers with a range of data storage services that follow advanced industry standards for data security lifecycle management using excellent technologies, practices, and processes in authentication, rights management, access control, data isolation, transmission security, storage security, data deletion, and physical destruction. It also ensures that tenant privacy, ownership and control over their data are not infringed upon, providing users with the most effective data protection.
12	Source code reviews	FIs should ensure confidentiality and integrity of source codes, other code artefacts (e.g. compiled and non-compiled codes, libraries, runtime modules), and review the source code during release management.	Customers should establish a mechanism for source code security management. To meet customer compliance requirements, HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding. All cloud services pass multiple security tests before release. The test environment is isolated from the production environment and avoids production data or unsensitized production data for testing, which needs to be cleaned up after use.
13	Penetration testing	CSP penetration test reports can be used to ensure the security of	Customers should conduct penetration testing of The CSP's environment. To meet customer compliance

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the underlying system, and to ensure that the test covers all systems involved in the service provision so that vulnerabilities are assessed, tracked, and properly managed/handled. An FI should consider using a Red Teaming approach to test the CSP's environment. It is also recommended that testing is performed on live systems subject to safety protocols to prevent any disruption of service.	requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services. Together with partners, HUAWEI CLOUD has launched host intrusion detection, web application firewall, host vulnerability scanning, web page anti-tampering, and penetration test services, which enhance the security detection, correlation, and protection capabilities of HUAWEI CLOUD.
14	Security events monitoring	Secure and robust security logging infrastructure should be leveraged. Consolidation of logs to a centralized system should be in place to ensure that the integrity and availability of the logs are maintained. The FIs should ensure that CSPs have snapshots of critical databases or systems of	Customers should establish a centralized monitoring platform to automatically analyze the security logs of each system, and timely detect and respond to security events. To meet customer compliance requirements, HUAWEI CLOUD has a centralized and complete log audit system. The system collects the management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems. HUAWEI CLOUD log management system is based on ELK. Moreover, HUAWEI CLOUD uses big data security analysis system, associates alarm logs of various security devices, carries out unified analysis, quickly and comprehensively identifies attacks that have occurred, and anticipates threats that have not yet occurred. The Relational Database Service (RDS) allows tenants to rapidly provision

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		record for disaster recovery/business continuity.	different types of databases whose compute and storage resources can flexibly scale to meet tenant service requirements. Automatic backup, database snapshot, and restoration functions are provided to prevent data loss.
15	Securing logs and backup	FIs and CSPs should take appropriate measures to protect the log data generated by the system, ensure the confidentiality and integrity of the log data, and ensure that the log data does not contain sensitive information.	HUAWEI CLOUD Trace Service (CTS) provides operating records of cloud service resources for users to query, and for auditing. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within Huawei's cloud system. CTS inspects the log data sent by various services to ensure that the data itself does not contain sensitive information in the following; • In the transmission phase, it ensures 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. Additionally, HUAWEI CLOUD manages behavioral logs for all physical devices, networks, platforms, applications, databases, and security systems, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days.
Run the Cloud (on-going basis)			

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
1	Change management	Ensure that all the changes follow a robust change management process that provides oversight commensurate with their risk. This includes changes controlled by the CSP for IaaS, PaaS and SaaS environments. Ensure oversight of major changes that could impact the stability and/or security of the cloud operating environment, and detection unauthorized or erroneous changes.	Customers should establish formal change management procedures. HUAWEI CLOUD provides Cloud Trace Services (CTS) to provide customers with operational records of cloud service resources for user query, audit, and backtracking. The actions of all people can be recorded in real time and systematically so that customers can perform audits of changes. HUAWEI CLOUD, as CSP, is responsible for the management of the infrastructure it provides and the various cloud services of IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a comprehensive change management process and regularly reviews and updates it. Define the change category and change window, as well as the change notice mechanism, depending on the extent to which the change may affect the business. The process requires that all change requests be submitted to the HUAWEI CLOUD change committee after the change manager makes a judgment. After the review, the network can be changed according to the plan. All changes need to be fully validated before application with tests such as production environment tests, gray release tests, and blue-green deployment. This ensures that the change committee has a clear understanding of the change, the timeframe, the possible rollback of the change, and all possible impacts.
2	Configuration management	FIs should implement monitoring to detect unauthorized changes to the cloud environment. Where possible, FIs should implement automated recovery to mitigate high risk changes.	Customers should monitor their changes to detect unauthorized changes. HUAWEI CLOUD provides Cloud Trace Services (CTS) to record operator changes to resources and system configurations on the China-made cloud for user query, and for auditing. HUAWEI CLOUD, as CSP, is responsible for the configuration management of the infrastructure it provides and various cloud services for IaaS, PaaS, and SaaS. The HUAWEI CLOUD Settings Configuration Manager manages all business units, including extraction of configuration models (configuration item types, various

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			configuration item attributes, relationships between configuration items, etc.), and recording configuration information. The relationship between configuration items, the properties of configuration items, and their use is managed through a professional configuration management database (CMDB) tool.
3	Events management	Define and monitor critical events to ensure that the confidentiality, availability, and integrity of the cloud environment are not compromised. Provide early detection of network and system anomalies in the information technology environment in order to respond to potential technical and security incidents in a timely manner, and manage and report incidents appropriately according to the critical degree of incidents and the allocated ownership.	Customers should develop critical incident management procedures to ensure that major incidents are detected and resolved quickly to ensure the safe and stable operation of the cloud environment. HUAWEI CLOUD Eye Service (CES) provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. CES provides real-time alarm monitoring, notifications, and personalized report views to accurately grasp the status of business resources. Users can set alarm rules and notification strategies independently, so that users can detect abnormal cloud resources promptly and take countermeasures. HUAWEI CLOUD, as a CSP, is responsible for the management of infrastructure and major events of various cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has a centralized and complete log audit system. The large data security analysis system is used to correlate alarm logs of various security devices and conduct unified analysis to quickly and comprehensively identify attacks, and predict attacks that have not yet occurred. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status.
4	Incident and problem management	Provide a reasonable level of security event	Customers should establish formal incident and issue management procedures.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		traceability detection in the information technology environment when a new threat to information is available. Ensure that technical and safety incidents are properly upgraded, and inform relevant stakeholders to take management measures. Ensure that events in the environment are properly reviewed and that gaps identified are corrected to prevent recurrence.	HUAWEI CLOUD Eye Service (CES) provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures. At the same time, HUAWEI CLOUD can also provide an anti-DDoS service, cloud WAF service, **Database Security Service (DBSS)**, and Cloud Trace Service (CTS) to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application-level and data-level attacks, as well as reviewing and auditing incidents. At the same time, HUAWEI CLOUD, as a CSP, is responsible for the event and change management of its infrastructure and various cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a complete event and management process to regularly review and update it. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source.
5	Capacity management	FIs should have a clear view of its requirements to operate its resources to ensure that business functions can proceed without any	Customers should establish formal capacity management procedures to monitor their cloud resources to ensure that they meet the needs of business growth. Customers pass through the HUAWEI CLOUD Eye Service (CES) which provides three-dimensional monitoring of flexible cloud servers, bandwidth, and

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		interruptions. Proper monitoring of resources to understand average utilization and peak value. Ensure that the system has appropriate resources to recover in case of failure or unplanned downtime.	other resources. The monitoring object of CES is the resource usage data of infrastructure, platform, and application services and does not monitor or access tenant data. CES can currently monitor the following indicators of cloud services: Elastic Computing Service (ECS), Elastic Volume Service (EVS), Virtual Private Cloud Service (VPC), Relational Database Service (RDS), Distributed Caching Service (DCS), Distributed Message Service (DMS), Elastic Load Balancing (ELB), Elastic Scaling Service (AS), Web Application Firewall (WAF), Host Vulnerability Detection Service (HVD), Cloud Desktop Service (Workspace), Machine Learning Service (MLS), Web Tamper Protection Service (WTP), Data Warehouse Service (DWS), Artificial Intelligence Service (AIS), and so on. These metrics allow users to set alert rules and notification policies to keep abreast of the health and performance of instance resources for each service. HUAWEI CLOUD has also developed a complete performance and capacity management process through early identification of resource requirements, and overall management of platform resource capacity and equipment inventory, HUAWEI CLOUD can continuously optimize resource utilization and resource availability levels, and ultimately ensure that cloud resources meet the business needs of users.
6	Patching and vulnerability management	Ensure that all assets in the cloud environment have clear ownership and are rated for their importance. Identify potential vulnerabilities and system instability quickly and safely, and deploy security	Customers should establish formal asset management procedures, classify their assets, and define asset owners to quickly identify and fix vulnerabilities in assets. 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 exposure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools (regardless of whether they are

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and operating system patches quickly.	found in Huawei or third party technologies) are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation, and its impact to our customers' services. To protect end users and tenants, HUAWEI CLOUD upholds the principle of responsible disclosure. It ensures no undue risks for potential exploitation and attacks will result from the disclosure of any vulnerability, HUAWEI CLOUD continues to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and tenants vulnerability mitigation solutions, standing shoulder to shoulder with our customers to tackle security challenges caused by vulnerabilities.
7	Collaborative disaster recovery testing	FIs should develop business continuity plans for key business functions and carry out their own simulated disaster recovery tests, which should be tested in conjunction with CSP as far as possible. CSP should develop disaster recovery and business continuity plans and, where appropriate, share them with financial institutions. Ensure that the continuing availability of services is commensurate with their critical level in the cloud	Customers should establish their own mechanisms for business continuity and develop RTO and RPO metrics to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate. To meet customer compliance requirements, HUAWEI CLOUD not only provides high-availability infrastructure, redundant data backup, and disaster preparedness in available areas, but has also obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		environment. Ensure that data, systems and applications can be recovered within the time frame required by financial institutions.	

10 How HUAWEI CLOUD Can Help Customers to Meet the Requirements of MAS Business Continuity Management Guidelines

The Business Continuity Management Guidelines issued by MAS on 6 June 2022 provides guidance for Singapore's FIs to strengthen business continuity management and aims to help FIs increase their resilience to service disruptions while minimizing the negative impact of service disruptions. This document covers several areas including Critical Business Services and Functions, Service Recovery Time Objective, Dependency Mapping, Concentration Risk, Continuous Review and Improvement, Testing, Audit, Incident and Crisis Management and so on.

The following summarizes the requirements for cloud service providers in the Business Continuity Management Guidelines and explains how HUAWEI CLOUD is assisting customers to meet these requirements.

10.1 Critical Business Services and Functions

The Business Continuity Management Guidelines notes that business functions underpin the provision of business services to an FI’s customers. When a business function is disrupted, all the business services that are dependent on it could be disrupted. Section 2 of this document sets out specific control requirements for critical business services and functions to enable FIs to identify and restore their critical business services and functions as quickly as possible in the event of disruptions. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2	Business Continuity and Disaster Recovery Plan Management	FIs should prioritize the recovery of its business services and functions based on their criticality, and determine the appropriate recovery strategies and	Customers should prioritize and properly allocate resources for recovery of critical business services and functions. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		resource allocation.	system that meets its business characteristics and has obtained the ISO 22301 certification. Based on the requirements of the system framework, HUAWEI CLOUD periodically analyzes the service impact, identifies critical services, determines the recovery objectives, minimum recovery levels, and recovery priorities of critical services, and determines the support resources required for recovery. In addition, HUAWEI CLOUD will identify the risks brought by the disruption to the organization, perform systematic analysis, and confirm risk handling measures. Based on the business impact analysis and risk assessment results, HUAWEI CLOUD will formulate appropriate recovery policies for critical resources of critical service processes, including personnel, sites, devices, third parties, and information systems.

10.2 Service Recovery Time Objective

The Business Continuity Management Guidelines notes that the Service Recovery Time Objective (SRTO), being a time-based metric, provides clarity within the FI on the expected recovery timelines for each business service. Section 3 of this document sets out specific control requirements for the determination of SRTO, which will help to guide the prioritization of resources during planning, and facilitate decision-making and monitoring of the recovery progress in a disruption. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.1 3.2	Business Continuity and Disaster Recovery Plan Management	FIs should establish their own business continuity mechanisms and formulate RTO and RPO indicators to ensure the continuity of critical services.	Customers should establish their own business continuity mechanism and ensure the RTO and RPO. HUAWEI CLOUD has established a comprehensive business continuity management system in compliance with the ISO22301 international standard for business continuity management. Based on the requirements of the system framework, HUAWEI CLOUD

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			periodically analyzes the service impact, identifies critical services, and determines the recovery time objective, recovery point objective, and minimum recovery level of critical services. When identifying critical services, HUAWEI CLOUD regards the impact of service interruption on customers as an important criterion for determining critical services.
3.3	Business Continuity and Disaster Recovery Plan Management	FIs should set out clearly defined criteria for BCP activation when a critical business service encounters partial disruption.	Customers should specify the start-up and recovery criteria for their business continuity plan when a critical business service encounters partial disruption. HUAWEI CLOUD has established a comprehensive business continuity management system in compliance with the ISO22301 international standard for business continuity management. Based on the requirements of the system framework, HUAWEI CLOUD formulates emergency classification standards, defines emergency levels, and determines emergency judgment cases. HUAWEI CLOUD classifies incidents into levels I, II, and III. Level III security incidents cover partial interruptions, such as common system faults, but do not affect the overall system running but slightly affect services or functions. HUAWEI CLOUD specifies risk tolerance and handling measures for emergencies of different levels to avoid, reduce, or transfer risks caused by emergencies and ensure the continuity of HUAWEI CLOUD services.

10.3 Dependency Mapping

The Business Continuity Management Guidelines notes that the financial sector has become increasingly interconnected with the growing reliance on common IT systems and third parties. Section 4 of this document sets out specific control requirements to mitigate the risks arising from these linkages and ensure the business continuity. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.4	Business Continuity and Disaster Recovery Plan Management	FIs should put in place measures that enable third parties to meet the SRTOs of its critical business services. This can be done through measures, such as the following: (a) establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations and support the FI's BCM; (b) review the BCPs of third parties and verify that the BCPs meet appropriate standards and are regularly tested; (c) establish arrangements with third parties to safeguard the availability of resources, such as requesting for dedicated manpower; (d) conduct audits on the third parties; or (e) perform joint tests with third parties.	Customers should take effective measures to enable the third party to meet the SRTO for critical business services. HUAWEI CLOUD provides the online HUAWEI CLOUD User Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level provided and HUAWEI CLOUD's responsibilities. In addition, HUAWEI CLOUD has developed offline contract templates that can be customized based on customer requirements. HUAWEI CLOUD will comply with the requirements specified in the agreement with the customer. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with the customer in monitoring and risk assessment of HUAWEI CLOUD. If FIs need HUAWEI CLOUD to participate in its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the FIs.
4.5	Business Continuity and Disaster Recovery Plan Management	FIs should put in place plans and procedures to address any unforeseen disruption, failure or termination of third-party arrangements.	Customers should have an effective business continuity plan in place to address service disruptions caused by third parties. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the ISO 22301 certification. Based on the

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			requirements of this system framework, HUAWEI CLOUD regularly formulates emergency plans for different product types, including basic services, operation centers, data centers, and organizations, and performs drills in different scenarios to maintain the effectiveness of the continuity plan. When the organization and environment of HUAWEI CLOUD change significantly, the effectiveness of service continuity will be tested.
4.6	Business Continuity and Disaster Recovery Plan Management	FIs should put in place measures to address the disruption of common utility services supporting critical business services, such as implementing redundancy or alternative contingency arrangements.	Customers should put in place measures to address the disruption of common utility services supporting critical business services. HUAWEI CLOUD can flexibly replace compute instances and storage data in multiple regions or among AZs in the same region. Each AZ is an independent fault maintenance domain. That is, AZs are physically isolated. In addition, each AZ has its own independent UPS and on-site backup power generation equipment. Each AZ is connected to a different power grid. All AZs are redundantly connected to multiple tier-1 transmission providers to further eliminate the risk of single points of failure. 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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			customers' applications enable N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. In addition, HUAWEI CLOUD provides customers with Storage Disaster Recovery Service (SDRS), Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Dedicated Distributed Storage Service (DSS) services to meet organizations' requirements for information security and information security management continuity in the event of a disaster, which will enable customers to perform disaster recovery. SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide high-level data reliability and service continuity. SDRS helps protect service applications. It replicates ECS data and configuration information to the DR site and allows servers where service applications are located to start and run properly from another location during downtime, improving service continuity.

10.4 Concentration Risk

The Business Continuity Management Guidelines notes that FIs may be exposed to concentration risk when several of its critical business services and/or functions are outsourced to a single service provider. Section 5 of this document sets out specific control requirements to mitigate the concentration risk. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.2	Cloud service security	FIs may consider segregating primary and secondary sites of critical business services and functions, or infrastructure (such as data centres) into different zones to	HUAWEI CLOUD can flexibly replace compute instances and storage data in multiple regions or among AZs in the same region. Each AZ is an independent fault maintenance domain. That is, AZs are physically isolated. In addition, each AZ has its own independent UPS and on-site backup power

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		mitigate wide-area disruption.	generation equipment. Each AZ is connected to a different power grid. All AZs are redundantly connected to multiple tier-1 transmission providers to further eliminate the risk of single points of failure. 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 N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. In addition, HUAWEI CLOUD provides customers with Storage Disaster Recovery Service (SDRS), Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Dedicated Distributed Storage Service (DSS) services to meet organizations' requirements for information security and information security management continuity in the event of a disaster, which will enable customers to perform disaster recovery. SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide high-level data reliability and service continuity. SDRS helps protect service applications. It replicates ECS data and configuration information to the DR site and allows servers where service applications are located to start and run properly from

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			another location during downtime, improving service continuity.

10.5 Continuous Review and Improvement

The Business Continuity Management Guidelines notes that BCM is an ongoing effort to ensure that the measures put in place are able to address operational risks posed by the latest threats, as well as plausible threats in the future. Section 6 of this document sets out specific control requirements for FIs to continuously review and improve their business continuity. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.1	Business Continuity and Disaster Recovery Plan Management	FIs should establish their own business continuity mechanism, set RTO and RPO indicators to ensure the continuity of their critical services, and regularly test and evaluate business continuity plans and disaster recovery plans.	Customers should establish a business continuity mechanism, specify the RTO and RPO, and periodically test the business continuity plan and disaster recovery plan. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its business characteristics, and has obtained the ISO 22301 certification. To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the weaknesses found in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective.
6.3	Security Monitoring	FIs should actively monitor and identify external threats and developments that could disrupt its normal operation, and have an escalation process to alert internal stakeholders	Customers should collect and analyze threat intelligence through different channels to identify, detect, and notify external threats. HUAWEI CLOUD continues to pay attention to the industry-renowned vulnerability database, security forums, email lists, and security conferences to ensure that HUAWEI

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and senior management about the relevant threats in a timely manner.	CLOUD-related vulnerability information is detected in a timely manner. In addition, HUAWEI CLOUD uses the situational awareness analysis system to associate alarm logs of various security devices and analyze them in a unified manner. Based on the big data analysis and high-accuracy threat intelligence database, HUAWEI CLOUD monitors threats on the cloud in real time, analyzes threat attacks, provides alarm notifications in a timely manner and presets response policies for typical threat incidents. HUAWEI CLOUD has formulated and implemented security incident grading standards and escalation processes. On the one hand, HUAWEI CLOUD clearly classifies security incidents and defines security incidents of each level. On the other hand, if a security incident occurs, HUAWEI CLOUD will obtain related information and grade the incident based on the rating criteria. If a security incident reaches a higher level during handling, HUAWEI CLOUD will update the level in real time and handle the incident. In addition, HUAWEI CLOUD specifies the time limit and scope of reporting security incidents at different levels. When a security incident occurs, HUAWEI CLOUD will notify the responsible personnel and management personnel of the incident within the specified time.
6.5	Business Continuity and Disaster Recovery Plan Management	FIs should regularly test and evaluate business continuity plans and learn lessons from security incidents to strengthen their business continuity preparedness.	Customers should periodically evaluate and test the business continuity plan and improve it. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its service characteristics, and has obtained the ISO 22301 certification.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the deficiencies identified in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective. In addition, HUAWEI CLOUD regularly collects statistics on incidents and analyzes the trend, finds out the root cause, and formulates solutions to prevent such incidents from occurring.
6.7	Business Continuity and Disaster Recovery Plan Management	FIs should periodically test and evaluate business continuity and disaster recovery plans and update them as appropriate as their operational environment and threat landscape changes.	Customers should periodically evaluate and test the business continuity plan and improve it. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its service characteristics, and has obtained the ISO 22301 certification. To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the deficiencies identified in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective. In addition, HUAWEI CLOUD regularly collects statistics on incidents and analyzes the trend, finds out the root cause, and formulates solutions to prevent such incidents from occurring.

10.6 Testing

The Business Continuity Management Guidelines notes that testing is crucial in validating an FI’s BCM preparedness. Section 7 of this document sets out specific control requirements to guide FIs in testing business continuity. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.1	Business Continuity and Disaster Recovery Plan Management	FIs should conduct regular and comprehensive testing to gain assurance that its response and recovery arrangements are robust, and enable them to continue the delivery of critical business services and functions in a timely and reliable manner following a disruption.	Customers should periodically test the business continuity plan to ensure its effectiveness. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the ISO 22301 certification. Based on the requirements of this system framework, HUAWEI CLOUD regularly formulates emergency plans for different product types, including basic services, operation centers, data centers, and organizations, and performs drills in different scenarios to maintain the effectiveness of the continuity plan. When the organization and environment of HUAWEI CLOUD change significantly, the effectiveness of service continuity will be tested.
7.2	Business Continuity and Disaster Recovery Plan Management	FIs should plan its test activities to meaningfully test all aspects of its BCM framework, and to meet the following test objectives: (a) validate and measure the effectiveness of the BCPs using appropriate metrics, and remediate any gaps or weaknesses that are identified in the recovery process; (b) familiarise personnel, including those of relevant third parties, involved in business continuity and crisis management with their roles and responsibilities. This includes how the alternate sites and recovery	

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		arrangements should be operated, so as to improve coordination and ensure a seamless execution of various plans; (c) sensitise senior management and staff involved in crisis management to the potential areas of concern that could arise in crisis situations, and practise making decisions under simulated conditions, including scenarios that require prioritizing the recovery of competing critical business services and functions; (d) stress test BCPs under severe but plausible scenarios to allow the FI to challenge its current planning assumptions and ensure the relevance and effectiveness of its BCPs, to better mitigate the impact of severe disruptions; and (e) verify that the SRTOs of its critical business services and RTOs of its critical business functions can be met through the established recovery strategies.	
7.3	Business Continuity and Disaster Recovery Plan Management	FIs should select the types of tests that best meet these objectives, and set out the frequency and scope	

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		of these tests to be commensurate with the criticality of the business services and functions. FIs should also properly document all its test records. Gaps and weaknesses identified from the FIs' business continuity testing should be reported to the senior management.	
7.4	Business Continuity and Disaster Recovery Plan Management	FI should establish a formal process to follow up on the remedial actions identified in each test.	Customers should follow up and document remediation activities against the business continuity plan. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its service characteristics, and has obtained the ISO 22301 certification. To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the deficiencies identified in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective. In addition, HUAWEI CLOUD regularly collects statistics on incidents and analyzes the trend, finds out the root cause, and formulates solutions to prevent such incidents from occurring.

10.7 Audit

The Business Continuity Management Guidelines notes that BCM audit is an important means to provide the FI with an independent assessment on the adequacy and effectiveness of the implementation of its BCM framework. Section 8 of this document sets out specific control requirements for auditing the business continuity of FIs. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
8.2	Assessment and Audit	FIs should audit its overall BCM framework and the BCM of each of its critical business services at least once every three years.	Customers should regularly (at least once every three years) audit their business continuity management framework and associated work. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its service characteristics, and has obtained the ISO 22301 certification. To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the deficiencies identified in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective. In addition, HUAWEI CLOUD will comply with the requirements specified in the agreement with the customer. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with the customer in monitoring and risk assessment of HUAWEI CLOUD.
8.4	Business Continuity and Disaster Recovery Plan Management	FIs should establish processes to track and monitor the implementation of sustainable remedial actions in response to the audit findings. FIs should escalate any significant audit findings on lapses that may have severe impact on the FI's BCM to the Board and senior management. FIs should submit the	Customers should follow up and remediate remediation activities against the business continuity plan. In addition, customers should communicate the results of audits that have significant impact to the Board and senior management. Also, Customers should submit the BCM audit reports to MAS upon request. HUAWEI CLOUD has comprehensive business continuity management policies and processes, developed a business continuity management system that meets its service characteristics, and has obtained the ISO 22301 certification.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		BCM audit reports to MAS upon request.	To ensure the suitability, adequacy, and effectiveness of business continuity, HUAWEI CLOUD regularly reviews its business continuity system to evaluate its procedures and capabilities. HUAWEI CLOUD will correct, record, analyze, and improve the deficiencies identified in the review, and update the business continuity plan based on the review results to ensure that the business continuity plan is effective.

10.8 Incident and Crisis Management

The provisions of the Business Continuity Management Guidelines related to incident and crisis management are important aspects of ensuring business continuity for FIs. Section 9 of this document sets out specific control requirements for FIs to conduct incident and crisis management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.1	Security Incident Response	FIs should have robust processes to manage incidents in order to resume critical business services and functions within the stipulated SRTOs/RTOs. Where the delivery of a business service depends on multiple business functions, an overall coordinator should be appointed to coordinate incident management and recovery across affected functions.	Customers should establish a comprehensive security incident management process. HUAWEI CLOUD has developed a security event management mechanism, including a general security event response plan and process, and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities that are responsible for each activity during the incident response process. According to internal management requirements, HUAWEI CLOUD tests the information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the testing.
9.2	Security Incident Response	FIs should have in place: (a) a crisis	Customers should conduct effective crisis management activities. HUAWEI CLOUD has developed a

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		management structure, with clearly defined roles, responsibilities, reporting lines, and chain of command (including designating alternates to primary representatives); (b) a set of pre-defined triggers and criteria for timely activation of the crisis management structure; (c) plans and procedures to guide the FI on the course of actions and decisions to be made during a crisis; (d)tools and processes to facilitate timely updating and assessment of the latest situation to support decision-making during a crisis; (e) a list of all internal and external stakeholders to be informed when a critical business service is disrupted, as well as communications plans and requirements (i.e. drawer plans, notification criteria, notification timelines, update frequency, etc.) for each stakeholder; and (f) communication channels, including mainstream and social media, to effectively communicate with its stakeholders, including alternative	security event management mechanism, including a general security event response plan and process, and continuously optimized the mechanism. The security incident response process clearly defines the roles and responsibilities that are responsible for each activity during the incident response process. According to internal management requirements, HUAWEI CLOUD tests the information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the testing. HUAWEI CLOUD log big data analysis system can quickly collect, process, and analyze massive logs in real time. The system collects management behavior logs of physical devices, networks, platforms, applications, databases, and security systems, and threat detection alarm logs of security products and components. The system continuously monitors and analyzes security incidents in real time to detect security incidents in a timely manner. In addition, HUAWEI CLOUD has a 7 x 24 professional security incident response team and a corresponding security expert resource pool to handle security incidents. HUAWEI CLOUD periodically collects statistics and analyzes trends of security incidents. For security incidents, the problem handling team will find the root cause and formulate solutions to prevent such incidents from occurring. HUAWEI CLOUD will strictly record all related information and handling process during emergency handling. All process-related materials should be archived and kept by dedicated personnel. HUAWEI CLOUD has a professional security event management system to record

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		channels that can be used when the primary communication channel is unavailable.	and track the progress and handling measures of all information security incidents, analyze the impact of incident handling, and track and close security incidents in an end-to-end manner to ensure that the entire handling process is traceable. HUAWEI CLOUD reviews and summarizes the impact of security incidents and the handling process, and notifies and reports the impacted users and supervision departments as required. HUAWEI CLOUD has developed a comprehensive event management and customer notification process. If an event occurs on the underlying platform of HUAWEI CLOUD, related personnel will analyze the impact of the event based on the process. If the event has or will affect cloud service customers, HUAWEI CLOUD will start the notification mechanism. and notify the customer of the event. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and recommended measures to be taken by the customer.
9.4	Security Incident Response	FIs should ensure that communications to its external stakeholders are proactive, transparent, and factual. This will reassure stakeholders and maintain customer confidence during a disruption or crisis.	Customers should be proactive in communicating with external stakeholders. HUAWEI CLOUD has a 7 x 24 professional security incident response team and a corresponding security expert resource pool to handle security incidents. HUAWEI CLOUD reviews and summarizes the impact of security incidents and the handling process, and notifies and reports the impacted users and supervision departments as required. HUAWEI CLOUD has developed a comprehensive event management and customer notification process. If an event occurs on the underlying platform of HUAWEI CLOUD, related personnel will analyze the impact of the event

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			based on the process. If the event has or will affect cloud service customers, HUAWEI CLOUD will start the notification mechanism. and notify the customer of the event. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and recommended measures to be taken by the customer.
9.5	Security Incident Response	To facilitate timely public communications, the FIs should have a communications plan and prepare drawer media statements that cater to different scenarios and holding statements that can be released immediately in the event of a disruption. Where necessary, FIs should also coordinate with peer FIs through the relevant industry associations to achieve consistent messaging to the public in the event of a widespread disruption. FIs should also identify its designated spokesperson(s) who will be responsible to address the media and the public.	Customers should develop an effective internal and external communication plan and maintain good and adequate communication with all stakeholders. In addition, customers should designate a spokesperson to speak to the public. HUAWEI CLOUD has established multiple internal and external information communication channels to ensure effective communication between HUAWEI CLOUD internal employees and external cloud service customers. HUAWEI CLOUD ensures that the cyber security assurance system is implemented in all systems, regions, and throughout the process, and actively promotes communication with stakeholders such as governments, customers, partners, and employees to ensure that stakeholders can receive information about HUAWEI CLOUD cyber security in a timely and effective manner. To facilitate smooth external communication, HUAWEI CLOUD assigns dedicated personnel to keep in touch with administrative agencies, risk and compliance organizations, local authorities, and regulators and establish contact points. HUAWEI CLOUD will work closely with external stakeholders to share information to promote progress in cyber security.
9.6	Security Incident Response	FIs should ensure that MAS is notified as soon as possible, but	Customers shall notify the regulatory authorities of the security incident within the specified time.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		not later than one hour upon the discovery of incidents where business operations will be severely disrupted, or when the BCP is going to be activated in response to an incident.	To help customers report cyber security incidents to MAS, HUAWEI CLOUD sets up a 7 x 24 professional security incident response team and expert resource pool to disclose related incidents in a timely manner and notify customers in a timely manner according to laws and regulations. In addition, HUAWEI CLOUD implements emergency plans and recovery processes to minimize service impact.

11 How HUAWEI CLOUD Can Help Customers Meet the Requirements of MAS Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption issued by MAS on 1 June 2021 highlights some of the more common key risks and control measures that FIs should consider before adopting public cloud services, providing guidance for FIs to use public cloud services more securely and reduce related risks.

The following summarizes the requirements for cloud service providers in the Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption and explains how HUAWEI CLOUD is assisting customers to meet these requirements.

11.1 Shared Cyber Security Responsibilities

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption focuses on the division of cyber security responsibilities under public cloud services and points out the responsibilities of FIs and cloud service providers in public cloud services. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7	Contractual Agreement	While CSPs are responsible for “Security-of-the-Cloud”, FIs would be responsible for “Security-in-the-Cloud”. a) “Security-of-the-Cloud” refers to the security of the public cloud services under the CSPs’ responsibility. In an IaaS or PaaS arrangement, these would typically include the security of the underlying hardware, system software and the hypervisor. For SaaS, this would also include the	Customers should clearly define their cyber security responsibilities with CSPs. 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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		underlying security of the application software. b) “Security-in-the-Cloud” refers to the security of the cloud workloads under the FIs’ responsibility. In an IaaS or PaaS arrangement, these should typically include securing IT systems components such as applications, operating system and orchestration tools. In a SaaS arrangement, it would generally include managing user account privileges and data access rights.	security (For details, see "3. HUAWEI CLOUD Security Responsibility Sharing Model" in this compliance guide). 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. HUAWEI CLOUD cooperates with customers to meet compliance requirements. The online HUAWEI CLOUD Customer Agreement defines the security responsibilities of cloud service customers and HUAWEI CLOUD, while the HUAWEI CLOUD Service Level Agreement stipulates the service level provided by HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be negotiated with customers to meet their requirements. If necessary, HUAWEI CLOUD will actively cooperate with customer inspection and due diligence. HUAWEI CLOUD will arrange special personnel to actively cooperate with the customer during their due diligence. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. In addition, HUAWEI CLOUD employs professional third-party auditors to audit cloud computing products and services provided by HUAWEI CLOUD every year, and publishes audit reports in accordance with the format specified in the OSPAR template. After the report is formed, HUAWEI CLOUD will issue copies of audit reports to customers in the financial industry according to internal processes.
8	Contractual Agreement	FIs should be aware that while CSPs are responsible for “Security-of-the-Cloud”, in some cases, FIs may have shared responsibilities for managing the controls implemented by the CSPs.	
9	Contractual Agreement	FIs are reminded to ensure that the cyber security responsibilities of all contracting parties are clearly delineated in their outsourcing agreement with CSPs.	

11.2 Identity and Access Management

To effectively manage cloud security risks, Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption recommends that FIs implement identity access management and sets out a number of specific requirements to standardize identity access management mechanisms. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10	Identity and Access Management	FIs should enforce the principle of least privilege stringently when granting access to information assets in the public cloud.	Customers should establish authentication and access control management mechanisms to restrict and monitor privileges for accessing information assets. The principle of least privilege is strictly enforced when granting access against information assets in the public cloud. Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM), including support for password authentication, IAM also supports multi factor authentication as an option. 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. In addition, 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. To meet the compliance
11	Identity and Access Management	FIs should implement multi-factor authentication (MFA) for staff with privileges to configure public cloud services through the CSPs' metastructure.	
13	Identity and Access Management	FIs that are integrating public cloud workloads with an on-premise authentication service should adopt prevailing best practices in securing such implementations to minimise contagion risk.	

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access HUAWEI CLOUD's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. Administrators of HUAWEI CLOUD-related systems must first pass two-factor authentication before they can access the management plane through a springboard. All operations are logged and sent to the centralized log audit system in time. The audit system has a strong data retention and query capability to ensure that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD also has a dedicated internal audit department which will regularly audit the activities of the O&M process. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure 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. In addition, HUAWEI CLOUD has established a series of hierarchical certification system requirements, including internal

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			IT environment, system platform, middleware, network devices, application systems, and related technical requirements. All access is followed and granted based on the concept of least privilege. The bastion host provides two-factor authentication based on passwords and email verification codes to authenticate users. When a user accesses a HUAWEI CLOUD office subnet through the Internet, the user needs to perform two-factor authentication based on the registered device, account, and password.
12	Certificate and Key Management	Credentials used by system/application services for authentication in the public cloud should be changed regularly. If the credentials are not used, they should be deleted immediately.	Customers need to change or delete the credentials used for authentication on a regular basis. HUAWEI CLOUD provides customers with user account management and identity authentication suitable for enterprise-level organizational structure through 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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 such as passwords or mobile phone numbers. At the same time, when HUAWEI CLOUD O&M personnel access HUAWEI CLOUD Management Network for centralized management of the system, they need to use only identifiable employee identity accounts. 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. Employee account is used to log on VPN and access gateway to realize the deep audit of user login.
14	Cybersecurity Architecture	FIs using multiple public cloud services may need to centrally manage security policies over the use of different public cloud services and ensure that the policies are consistently enforced.	When multiple public cloud services are used, customers need to manage security policies for cloud services in a unified manner and ensure that they are effectively implemented. In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the public-facing network perimeter, trust boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities. HUAWEI CLOUD helps customers build a network security protection system to secure their cloud services. Customers at the Internet border can detect and clean abnormal traffic and traffic attacks by doing the following: deploying Anti-DDoS services; partitioning and isolating key network partitions through Virtual Private Cloud (VPC) and deployment of a Web Application Firewall (WAF) to deal with web attacks to protect web application services and systems deployed in the DMZ area that are oriented to the external network.

11.3 Securing Applications in Public Cloud

The security of applications in the public cloud is one of the concerns of this document. Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides a number of recommendations around how to secure applications in public clouds. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
16	Development Process Security	Where applications are developed for the public cloud environment, FIs are reminded to adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, conduct robust threat modelling, and implement prevailing best practices in software security (e.g. using Open Web	Customers should adopt appropriate Secure Software Development Lifecycle (SSDLC) processes and establish DevSecOps management mechanisms. HUAWEI CLOUD has pursued the new DevOps process, which features rapid and continuous iteration capabilities, and integrated the HUAWEI security development lifecycle (SDL). In addition, gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		Application Security Project "OWASP" guides and frameworks). Should FIs use a continuous development-operations process ("DevOps"), security should be embedded throughout the Continuous Integration/Continuous Development (CI/CD) toolchain. FIs should adopt DevSecOps, which is the practice of automating and integrating IT operations, quality assurance and security practices in their software development process.	capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. HUAWEI CLOUD hierarchically manages the development environment and implements protection measures such as physical isolation, logical isolation, access control, and data transmission channel approval and audit.
17	Identity and Access Management	When adopting a microservice architecture, FIs should ensure that adequate security controls are in place, including, securing the service discovery mechanism, using service mesh for fine-grain access control to APIs and implementing robust authentication for microservices.	Customers must implement effective security control measures to ensure security when using the microservice architecture. In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the public-facing network perimeter, trust boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities. HUAWEI CLOUD helps customers build a network security protection system to secure their cloud services. Customers at the Internet border can detect and clean abnormal traffic and

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			traffic attacks by doing the following: deploying Anti-DDoS services; partitioning and isolating key network partitions through Virtual Private Cloud (VPC) and deployment of a Web Application Firewall (WAF) to deal with web attacks to protect web application services and systems deployed in the DMZ area that are oriented to the external network.
18	Identity and Access Management	When securing APIs, FIs should implement fine-grain access control and adopt the principle of least privilege i.e. strictly limit access to services to what is needed only, with the minimum level of privileges needed. FIs should also enforce robust IAM to authenticate service requests. FIs should not rely on implicit trusts when granting access (e.g. allow access based on the static IP addresses of requestor).	Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM), including support for password authentication, IAM also supports multi factor authentication as an option. 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. In addition, 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. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access HUAWEI CLOUD's cloud management network to centralize the management of the system, employee identity account and two-

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			factor authentication are required. Administrators of HUAWEI CLOUD-related systems must first pass two-factor authentication before they can access the management plane through a springboard. All operations are logged and sent to the centralized log audit system in time. The audit system has a strong data retention and query capability to ensure that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD also has a dedicated internal audit department which will regularly audit the activities of the O&M process. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure 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. In addition, HUAWEI CLOUD has established a series of hierarchical certification system requirements, including internal IT environment, system platform, middleware, network devices, application systems, and related technical requirements. All access is followed and granted based on the concept of least privilege. The bastion host provides two-factor authentication based on passwords and email verification codes to authenticate users. When a user accesses a HUAWEI CLOUD office subnet through the Internet, the user needs to perform two-factor authentication based on the registered device, account, and password.

11.4 Data Security and Cryptographic Key Management

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption focuses on data security and cryptographic key management. It is recommended that FIs take appropriate data security measures and strengthen the cryptographic key management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
21	Data Security	FIs should implement appropriate data security measures to protect the confidentiality and integrity of sensitive data in the public cloud, taking into consideration data-at-rest, data-in-motion and data-in-use where applicable. a) For data-at-rest i.e. data in cloud storage, FIs may implement additional measures e.g. data object encryption, file encryption or tokenisation in addition to the encryption provided at the platform level. b) For data-in-motion i.e. data that traverses to and from, and within the public cloud, FIs may implement session encryption or data object encryption in addition to the encryption provided at the platform level. c) For data-in-use i.e. data that is being used or processed in the public cloud, FIs may implement confidential computing solutions if available from the	Customers should implement appropriate data security measures and consider industry-recognized encryption algorithms and key management mechanisms when using encryption to protect data. In addition, customers can manage keys in the hardware security module and host them in a secure environment. Customer shall also ensure that the cryptographic key management policies, standards, and procedures of the cryptographic key service provider adequately protect the security of the keys. HUAWEI CLOUD encapsulates complex data encryption and decryption, and key management logic. At present, cloud hard disk, object storage, image service, relational database and other services all provide data encryption (server-side encryption) function using high-intensity algorithm to encrypt the stored data. 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 ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, customer's master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		CSPs. Confidential computing solutions protect data by isolating sensitive data in a protected, hardware-based computing enclave during processing.	HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. 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.
22	Certificate and Key Management	FIs should consider adopting cryptographic key management strategies that accord them a high level of control and protection over cryptographic keys used for encrypting sensitive data.	
23	Certificate and Key Management	To secure cryptographic keys used for encrypting sensitive data, FI may consider generating, storing and managing the keys in a hardware security module (HSM) and hosting the HSM in an environment that the FI has a higher degree of control over.	
24	Certificate and Key Management	FIs should ensure that the CSPs' cryptographic key management policy, standards and procedures are adequate to protect the keys from unauthorised access, usage and disclosure throughout the cryptographic key management life cycle.	

11.5 Immutable Workloads and Infrastructure-as-Code

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides a number of recommendations for FIs for the use of immutable workloads and the use of "infrastructure as code" to configure or manage FIs' workloads in public clouds. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
25	Virtualization Security Capability	FIs may consider using immutable workloads to ensure the security and stability of workload components especially during software upgrades or security patching. For immutable workloads, server instances are replaced with updated images instead of being changed. Should a server instance be compromised, it could be replaced with a clean image quickly. Testing should be performed on immutable workloads images to ensure that an image is secure and stable before implementing in the production environment.	Customers can maintain the security and stability of workload-related components by using immutable workloads. To meet customers' regulatory requirements, HUAWEI CLOUD uses an integrity check mechanism to ensure the integrity of system parameters. For example, at the VM OS layer, HUAWEI CLOUD Image Management Service (IMS) supports image integrity check. When a VM is created based on an image, the system automatically checks the image integrity to ensure that the created VM contains complete image content. In addition, comprehensive change management procedures are provided to prevent HUAWEI CLOUD O&M personnel from modifying system configuration parameters without authorization.
26	Security Configuration Management	FIs using Infrastructure-as-Code (IaC) to provision or manage public cloud workloads should implement the necessary controls to minimise the risk of misconfiguration, and avoid using both IaC and non-IaC approaches concurrently in order to reduce the	When configuring or managing workloads in the cloud through Infrastructure as Code, customers should implement appropriate controls to secure the configuration and mitigate the related risks. Currently, HUAWEI CLOUD has established the O&M configuration management process guide. HUAWEI CLOUD manages the lifecycle of O&M configuration items and their relationships to ensure that configuration items in the O&M process are correctly identified

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		complexity of the IT environment. FIs should also ensure that IaC configuration files are protected from unauthorised access and modification.	and recorded, providing accurate and reliable configuration information and supporting secure, stable, and efficient operation of O&M services. HUAWEI CLOUD establishes unified baseline configuration standards for server operating systems, database management systems, and network devices that support service operation to implement unified management of service baseline configurations. In addition, HUAWEI CLOUD builds a configuration monitoring platform to monitor configuration items of server operating systems, database management systems, and network devices in real time. The monitoring platform compares the actual configuration items with the standard configuration baseline. When a difference occurs, the difference analysis result is automatically sent to the inspection administrator by email for follow-up handling. In addition, HUAWEI CLOUD periodically reviews the consistency between the existing firewall configuration policies and the implementation on the live network to rectify the identified differences.

11.6 Cyber Security Operations

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides a number of recommendations for FIs to conduct day-to-day cybersecurity operations. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
27	Security Monitoring	To maintain holistic cyber situational awareness of information assets, FIs should avoid performing security monitoring of on-	Customers should establish a centralized monitoring platform to automatically analyze security logs of each system and detect and respond to security events and events in a timely manner. To meet customer compliance

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		premise applications or infrastructure, and public cloud workloads in silo. FIs should feed cyber-related information on public cloud workloads into their respective enterprise-wide IT security monitoring services to facilitate continuous monitoring and analysis of cyber events.	requirements, HUAWEI CLOUD has a centralized and complete log audit system. The system collects the management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems. HUAWEI CLOUD log management system is based on ELK. Moreover, HUAWEI CLOUD uses big data security analysis system, associates alarm logs of various security devices, carries out unified analysis, quickly and comprehensively identifies attacks that have occurred, and anticipates threats that have not yet occurred. The Relational Database Service (RDS) allows tenants to rapidly provision different types of databases whose compute and storage resources can flexibly scale to meet tenant service requirements. Automatic backup, database snapshot, and restoration functions are provided to prevent data loss.
28	Security Incident Response	FIs should also ensure that their incident response, handling and investigation processes are adapted for public cloud workloads.	Customers should establish appropriate incident management procedures to resolve system and network failures in a timely manner. As a CSP, HUAWEI CLOUD manages key incidents of infrastructure and cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has a centralized and complete log audit system. The big data security analysis system is used to associate alarm logs of various security devices and analyze the logs in a unified manner, quickly and comprehensively identify attacks that have occurred and predict threats that have not occurred. HUAWEI CLOUD has a professional security incident response team to monitor alarms in real time. Key events that can be quickly identified, demarcated, isolated, and recovered based on the incident rating criteria, response time, and resolution time. Escalate and report events based on

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			the real-time status of events.

11.7 Cloud Resilience Risk Management

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption recommends that FIs assess and monitor the resilience of cloud services and take appropriate measures to ensure the resilience of cloud services. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
29	Cloud Infrastructure Security	FIs should evaluate the track records of the CSP in maintaining the resiliency of its public cloud services to verify that they are commensurate with the FIs' business needs. Such evaluation should be performed prior to engaging the service of a CSP, and on a regular basisafter engaging the CSP.	Customers should periodically assess the track record of the cloud service provider in maintaining the resilience of their public cloud services. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with FIs in supervision and investigation. At the same time, the customer should ensure that the cloud service provider has appropriate cloud redundancy or fault tolerance. 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 N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.
30	Cloud Infrastructure Security	For cloud workloads that require high availability, it is the FI's responsibility to ensure that the CSP has appropriate cloud redundancy or fault-tolerant capability and that the appropriate features are enabled for the cloud workloads. Cloud workloads could also be deployed in multiple geographically separated data centres to mitigate location-specific issues that may disrupt the delivery of public	

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		cloud services.	
31	Cloud Infrastructure Security	FIs should be proactive in monitoring the maintenance schedule, service disruptions, changes to services and end-of-life of services announced by the CSPs, such as via the CSPs' websites or through the cloud metastructure, so as to be able to take timely measures to ensure that FIs' systems remain available.	Customers should actively monitor information such as service interruptions published by cloud service providers so that appropriate responses can be taken. In addition, customers should establish a centralized monitoring platform to automatically analyze security logs of each system and detect and respond to security events and events in a timely manner. Customers can learn about cloud services provided by HUAWEI CLOUD on the HUAWEI CLOUD official website. HUAWEI CLOUD provides a unified hotline, email address, and work order system to process service requests from FIs. HUAWEI CLOUD will also establish contact with relevant regulatory authorities for necessary communication. To meet customer compliance requirements, HUAWEI CLOUD has a centralized and complete log audit system. The system collects the management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems. HUAWEI CLOUD log management system is based on ELK. Moreover, HUAWEI CLOUD uses big data security analysis system, associates alarm logs of various security devices, carries out unified analysis, quickly and comprehensively identifies attacks that have occurred, and anticipates threats that have not yet occurred. HUAWEI CLOUD Eye Service (CES) provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. CES provides real-time alarm monitoring, notifications, and personalized report views to accurately grasp the status of business resources. Users can set

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			alarm rules and notification strategies independently, so that users can detect abnormal cloud resources promptly and take countermeasures.

11.8 Outsourcing Due Diligence on CSPs

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides a number of recommendations for FIs to conduct due diligence on cloud service providers. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
32	Contractual Agreement	Some CSPs may offer FIs using public cloud services contractual terms and conditions that are tailored for the financial sector to enable the FIs to better meet their outsourcing due diligence, risk management and regulatory compliance needs. These terms and conditions may include the granting of audit and information access rights to FIs and their regulators for the purpose of performing outsourcing due diligence and carrying out supervisory reviews. In considering a cloud outsourcing arrangement, FIs should ensure that their ability to manage risk and meet regulatory requirements/expectationsis not impeded by contractual terms and	Customers should enter into outsourcing agreements with cloud service providers that specify requirements such as granting FIs and their regulators audit and access to information. To complement the customer's oversight of cloud service providers, HUAWEI CLOUD's online HUAWEI Cloud User Agreement defines the security responsibilities of cloud service customers and Huawei, and the HUAWEI CLOUD Service Level Agreement defines the level of services provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed an offline contract template, which can be negotiated based on customer requirements. HUAWEI CLOUD will arrange special personnel to actively cooperate with the customer during their due diligence. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		conditions.	
33	Assessment and Audit	FIs should ensure that independent audits and/or expert assessments of cloud outsourcing arrangements are conducted as part of their outsourcing due diligence and risk management.	Customers should conduct an independent audit and/or expert assessment of their cloud outsourcing arrangements. HUAWEI CLOUD can provide dedicated personnel to assist in the expert evaluation entrusted by customers and actively respond to and cooperate with customers' audit activities. In addition, HUAWEI CLOUD has obtained multiple international authoritative security and compliance certifications. HUAWEI CLOUD hires a professional third-party audit organization to audit the cloud computing products and services provided by HUAWEI CLOUD every year.

11.9 Vendor Lock-in and Concentration Risk Management

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides a number of recommendations for FIs to reduce the risks associated with vendor lock-in and concentration. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
35	Contractual Agreement	For cloud workloads that are critical to the FIs, exit strategies should be developed. The exit strategy could consider the pertinent risk indicators, exit triggers, exit scenarios, portability of the data and possible migration options.	Customers should develop an exit plan. During the destruction of customer data, HUAWEI CLOUD clears the specified data and all the copies. Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to ensure that data

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			on the storage medium cannot be restored. When the service agreement is terminated, HUAWEI CLOUD provides cloud data migration services (CDM) that support data migration between multiple types of data sources, such as databases, data warehouses, files, and so on, and between multiple environments to meet the needs of multiple business scenarios, such as data in the cloud, data exchange in the cloud, and data return to the local data center.

11.10 Skillset

Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption provides recommendations on the expertise and skills available to FI employees. The relevant control requirements and HUAWEI CLOUD's response are as follows:

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
37	Personnel Security Management	FIs should ensure that their cloud risk management strategy considers whether staff have the requisite expertise and experience to understand and manage the risks of public cloud adoption. In addition, FIs should ensure staff have the necessary knowledge and skillset to manage the attendant technology and cyber risks for different cloud services which are used in their organisations.	Customers should ensure that employees have the necessary knowledge and skills to handle risks related to the public cloud. HUAWEI CLOUD has established a series of cybersecurity training and learning mechanisms to ensure that employees' information security awareness meets the company's requirements. Employees are required to continuously learn about cybersecurity, understand relevant policies and systems, know what they should and shouldn't do, and commit to implementing them as required.

12 Conclusion

This user guide describes how HUAWEI CLOUD provides customers with cloud services that meet Singapore's regulatory requirements of the financial industry, and shows that HUAWEI CLOUD complies with key regulatory requirements issued by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS). This aims to help customers learn more about HUAWEI CLOUD's compliance with Singapore's financial industry regulatory requirements to assure customers that they can store and process customer content data securely through HUAWEI CLOUD services. To some extent, this document also guides customers on how to design, build, and deploy a secure cloud environment that meets the regulatory requirements of Singapore's financial industry on HUAWEI CLOUD, and helps customers better shoulder security responsibilities together with HUAWEI CLOUD.

This user guide is for reference only and does not have legal effect or constitute legal advice. Customers should assess their use of cloud services as appropriate and ensure compliance with the relevant Singapore financial industry regulatory requirements when using HUAWEI CLOUD.

13 Change History

Released On	Version	Description
January 2023	3.0	Compliance requirement update.
April 2022	2.0	Compliance requirement update.
March 2021	1.1	Compliance requirement update.
November 2019	1.0	This issue is the first official release.