HUAWEI CLOUD Compliance with Singapore Financial Services Regulations & Guidelines

Issue 02

Date 2021-03-22

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

In the recent wave of technological development, more and more financial institutions (FIs) are seeking to transform their businesses. They want to leverage advanced technologies to reduce costs, improve operational efficiency, and innovate their business models. To standardize the use of the information technology in the financial industry, the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) have released a series of regulatory requirements, guidelines, and notices. These requirements address risk management, outsourcing management, and cloud computing implementation of FIs in Singapore.

HUAWEI CLOUD is committed to helping FIs meet these regulatory requirements and continuously providing FIs with cloud services and business operating environments that meet industrial standards. This document describes how HUAWEI CLOUD will assist Singapore FIs in meeting the regulatory requirements in the following guidelines and notices 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. These 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.

2 HUAWEI CLOUD Security and Privacy Compliance

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of international and industry security compliance certifications[1], ensuring the security and compliance of businesses deployed by cloud service customers.

HUAWEI CLOUD has attained the following certifications:

Certification	Description
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
Classified Cybersecurity Protection of China's Ministry of Public Security	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.

Certification	Description
Singapore MTCS Level 3 Certification	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
ISO 20000-1:2011	ISO 20000 is an international recognized information technology service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure CSPs can provide effective IT services to meet the requirements of customers and businesses.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Gold Certification	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.

Certification	Description
Gold O&M (TRUCS)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification - Cyberspace Administration of China (CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.
International Common Criteria EAL 3+ Certification	Common Criteria (CC) certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed CC EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is an international code of conduct that focuses on the protection of personal data in the cloud. The adoption of ISO 27018 indicates that HUAWEI CLOUD has met the requirements of an internationally complete personal data protection and management system.

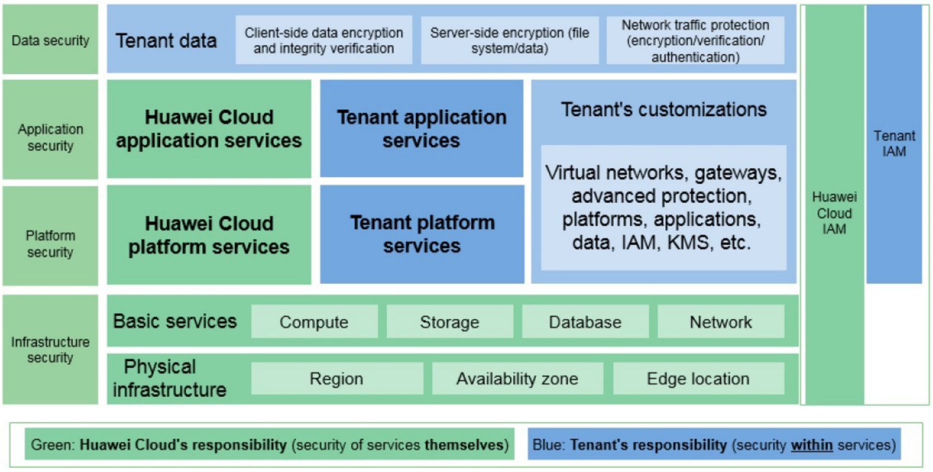
Certification	Description
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.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

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
Client-side data encryption and integrity verification
Server-side encryption (file system/data)
Network traffic protection (encryption/verification/ authentication)
Application security
Huawei Cloud application services
Tenant application services
Tenant's customizations
Virtual networks, gateways, advanced protection, platforms, applications, data, IAM, KMS, etc.
Platform security
Huawei Cloud platform services
Tenant platform services
Huawei Cloud IAM
Tenant IAM
Infrastructure security
Basic services
Compute
Storage
Database
Network
Physical infrastructure
Region
Availability zone
Edge location
Green: Huawei Cloud's responsibility (security of services themselves)
Blue: Tenant's responsibility (security within services)

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 Meets 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 Guidelines mainly cover the risk management practices of FIs, the guidelines for FIs to select cloud service providers, and the requirements for using cloud services. 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 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. This covers the responsibilities 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, and so on. 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.4	Assessment of service providers	In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due 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.	Customers should conduct due diligence to identify the risks of their outsourcing arrangements with service providers. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence by FIs. 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 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	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 specific customer needs. For more information, please refer to *HUAWEI CLOUD Customer Agreement.*

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 and sustainable security infrastructure and services to our customers. We will also openly and transparently tackle cloud security challenges standing

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			should-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.*

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.7	Business continuity manageme nt	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 emergency drills and tests, to continuously optimize emergency response.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD 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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

5.2 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 Meets the Requirements in MAS Technology Risk Management Guidelines

The *Technology Risk Management Guidelines* issued by the MAS stipulate the management principles and best practice standards of FIs on technology risks to guide Singapore's FIs in establishing a sound and reliable technology risk management framework, enhancing the security, reliability, flexibility and recoverability of the business systems, and protecting customer data and transactions and information systems. *Technology Risk Management Guidelines* cover requirements of the board of directors and senior management on technology risk management, outsourcing IT risk management, IT system acquisition and development, system reliability, availability and recoverability, operational security management of infrastructure, data center protection and control, and access control.

The following summarizes compliance requirements for cloud service providers in the *Technology Risk Management Guidelines* and explains how HUAWEI CLOUD assists FIs in meeting their requirements.

6.1 Oversight of Technology Risks by Board of Directors and Senior Management

Chapter 3 of the *Technology Risk Management Guidelines* 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 board roles and responsibilities, employee selection processes, IT policies, standards, and procedures, and IT security awareness. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.3	People selection process	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.
3.4	IT security awareness	All contractors and suppliers who have access to financial institution IT resources and IT systems should develop safety awareness training plans and implement or update them at least once a year.	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, 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 Management of IT Outsourcing Risks

Chapter 5 of the *Technology Risk Management Guideline* requires FIs to conduct inspection and due diligence on outsourced service providers and to give special consideration to cloud service providers. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.1	Due diligence	Before appointing service providers, financial institutions need to conduct due diligence to prove their feasibility, capacity, reliability and financial status. FIs should ensure that all contractual terms and conditions concerning the roles, relationships, obligations and responsibilities of the parties are stated in written agreements. Service providers should accept requests of relevant parties from financial institutions to view their systems, operations, documents and facilities. FIs should require service providers to obtain expert reports on the adequacy and compliance of the security of services provided and to regularly monitor and review them. FIs should require service providers to establish a disaster recovery emergency management framework that clearly records, maintains and tests the personnel responsibilities for contingency plans and recovery processes. Review, update, and test disaster recovery plans on a regular basis in accordance with changing technical conditions and operational requirements.	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 has developed a complete emergency contingency plan, which details the organization, procedures and operating norms of emergency response, and conducts regular tests to ensure the continuous operation of cloud services and the security of customer business and data.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.2	Cloud computing	FIs should ensure that cloud service providers can isolate and identify their customer data and other information system assets. FIs should have the right to delete or destroy data stored in the Service Provider's systems and backups when the contract with the service provider has expired or before it expires. Cloud service providers are also required to demonstrate to financial institutions the ability to restore outsourced systems and IT services within the stated Recovery Time Target (RTO).	Customers should establish their own business continuity mechanism and formulate RTO and RPO indicators to ensure continuity of key business. Customers can use HUAWEI CLOUD's data backup and archive service to minimize data loss in the event of a disaster. HUAWEI CLOUD has a comprehensive disaster recovery plan that regularly undergoes tests. HUAWEI CLOUD ensures that cloud services are running in the event of a disaster. Regarding data isolation, HUAWEI CLOUD recommends that data be distinguished and isolated at the beginning of the data life cycle by running a classification and risk analysis on the client's data. Based on the risk analysis results, clarify the storage location, storage services and security measures to protect data. When customers use cloud hard drive, object storage, cloud database, container engine and other services, HUAWEI CLOUD ensures that customers can only access their own data through different granularity access control mechanisms such as volume, bucket, database instance, container and so on. In the scenario of a customer self-built storage, for example, when installing database software on virtual machine instances, it is suggested that customers use HUAWEI CLOUD's **Virtual Private Cloud (VPC)** service to construct a private network environment, divide the network area through subnet planning, routing policy

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			configuration, place the storage in the internal subnet, and configure the network ACL and security group rules to access the subnet, as well as strictly controlling the network traffic of the virtual machine. When customers take the initiative to delete data or delete data due to the expiration of service, HUAWEI CLOUD will strictly follow the data destruction standard and the agreement with customers to remove stored customer data. For more information on data deletion, please refer to the *White Paper for HUAWEI CLOUD Data Security*.

6.3 Acquisition and Development of Information Systems

Chapter 6 of the *Technology Risk Management Guidelines* requires FIs to manage the acquisition and development of information systems, and identify defects in the system design, development and testing phases. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	Response of HUAWEI CLOUD
6.2	Security requirements and testing	The FI should maintain separate physical or logical environments for unit, integration, as well as system and user acceptance testing ("UAT"), and closely monitor vendor and developers' access to UAT environment.	When deploying a development environment, a test environment, and a production environment, customers should ensure that the physical and logical aspects of the environment are isolated and that access to the environment is strictly managed. Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled.

6.4 System Reliability, Availability and Recoverability

Chapter 8 of the *Technology Risk Management Guidelines* 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. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
8.3	Disaster recovery testing	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.

6.5 Operational Infrastructure Security Management

Chapter 9 of the *Technology Risk Management Guidelines* provides FIs with requirements for infrastructure security operations management, covering data loss prevention, technology refresh management, networks and security configuration management, vulnerability assessment penetration testing, patch management, and security monitoring. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
9.1	Data loss prevention	FIs should identify important data and adopt adequate measures to detect and prevent unauthorized access, copying or transmission of confidential information.	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 running first 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. For more details, please refer to the *White Paper for HUAWEI CLOUD Data Security*.

6.6 Data Centers Protection and Controls

Chapter 10 of the *Technology Risk Management Guidelines* requires FIs to ensure the security of their data centers, including threat and vulnerability risk assessment, physical security, data center resilience and other aspects. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
10.1	Threat and vulnerability risk assessment	FIs should assess the risks of threats and vulnerabilities according to the various possible situations of threats, considering factors such as the building structure of 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 assessment on global data centers to ensure that data centers strictly implement access control, security measures, routine monitoring and audit, emergency response and other measures. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities 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.

6.7 Access Control

Chapter 11 in the *Technology Risk Management Guidelines* requires FIs to take appropriate access control measures, including user access management and privileged access management. The following table describes relevant control requirements and HUAWEI CLOUD's responses.

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
11.1	User access management	Employees of vendors or service providers who are authorized to access to the FI's critical systems and other compute resources will pose similar risks as the FI's personnel. FIs shall subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.	Customers need to establish an identity authentication and access control management mechanism for the information system to control and monitor the access to the system. HUAWEI CLOUD provides **Identity and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to verify user identities through passwords or multi-factor authentication. IAM provides federation authentication for customers. Customers who have a reliable identity authentication service provider in place can map their federated users to IAM users in a specified period for access to customer's HUAWEI CLOUD resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. In addition, HUAWEI CLOUD provides **Cloud Trace Service (CTS)** for customers to collect, store, and query operation records of cloud resources for security analysis, compliance auditing, resource tracking, and fault locating. To meet customers' compliance requirements, HUAWEI CLOUD has established a comprehensive O&M and operation account management mechanism. O&M engineers are required to provide employee identity accounts and use multi-factor authentication when accessing the HUAWEI CLOUD management network to centrally manage the system. O&M accounts are centrally managed on the LDAP platform and automatically audited. This ensures that the entire process, including user creation,

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
			authorization, authentication, and permission reclaiming, is manageable. RBAC is implemented based on service dimensions and service responsibilities. O&M personnel can access devices within their authorization only.
11.2	Privileged access management	FIs shall closely monitor employees with privileged system access permissions, and record and review their system activities.	Customers need to establish a management mechanism to closely monitor the use of administrative accounts. To meet customers' compliance requirements, administrators of the HUAWEI CLOUD systems must pass the two-factor authentication before accessing the management plane through the jump server. Administrators' operations are logged and transferred to the centralized log audit system in a timely manner. The log audit system can keep logs for more than 180 days and ensure that logs within 90 days can be queried. HUAWEI CLOUD has a dedicated internal audit department that regularly audits all activities during O&M.

7 How HUAWEI CLOUD Meets the Requirements in MAS *Notice on Cyber Hygiene*

MAS issued 11 *Notices on Cyber Hygiene* on August 6, 2019 and November 5, 2019 for FIs. These notices provide practical guidance for FIs in Singapore on compliance with relevant acts. These notices cover administrative accounts, security patches, security standards, network perimeter defense, malware prevention, and multi-factor authentication.

The following summarizes the control requirements for cloud service providers in *Notice on Cyber Hygiene* and explains how HUAWEI CLOUD will help customers meet these control requirements.

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
4.1	Administrative accounts	FIs shall ensure that every administrative account for any operating system, database, application, security device, or network device is protected from being used for unauthorized access.	Customers need to establish a management mechanism to closely monitor the use of administrative accounts. HUAWEI CLOUD provides IAM and the privileged access management (PAM) function for customers to manage administrative accounts in an effective, fine-grained manner. HUAWEI CLOUD provides **CTS** for customers to record operations on cloud service resources so that they can query, audit, and backtrack operations. HUAWEI CLOUD implements role-based access control (RBAC) for O&M personnel. They can perform operations within authorization only. Administrative accounts and emergency accounts are granted to O&M personnel based on their responsibilities only. All applications for administrative or emergency accounts shall be reviewed and approved through multiple levels. HUAWEI CLOUD can log in to the management console or resource instances of a customer to assist the customer in maintenance only after HUAWEI CLOUD has been authorized by the customer (with the account and password provided by the customer).

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
4.2	Security patches	FIs shall establish a vulnerability management process and implement controls on every system, including installing and updating security patches in a timely manner. Banks shall establish mitigation and control measures to fix vulnerabilities that cannot be fixed by patches.	Customers need to establish a vulnerability management process and develop mitigation measures for vulnerabilities that cannot be fixed by patches. HUAWEI CLOUD provides **Vulnerability Scan Service (VSS)Vulnerability Scan Service (VSS)** for customers to scan for vulnerabilities on their websites, operating systems, asset compliance, and baseline configuration and weak passwords. VSS automatically discovers security risks of websites and servers to secure customer's business on the cloud from multiple dimensions. 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 customer businesses. For vulnerabilities that involve the cloud platform and customer businesses, HUAWEI CLOUD will push the vulnerability mitigation and recovery suggestions and solutions to end users and customers in a timely manner after making sure that no high attack risks will be caused by proactive disclosure. HUAWEI CLOUD

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
			will face the challenges brought by the security vulnerabilities together with customers.
4.3	Security standards	FIs shall establish a written set of security standards for every system and ensure compliance to the security standards. Mitigating controls should be implemented where the system is unable to conform to the security standards.	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.

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
4.4	Network perimeter defense	FIs shall implement controls at its network perimeter to restrict all unauthorized network traffic.	Customers need to divide and isolate security zones on their networks and strictly control access between different security zones. HUAWEI CLOUD leverages multi-layers security isolation, access control, and border protection technologies on its physical and virtual networks by considering network architecture design, device selection, and system O&M as well as implements required management and control measures to ensure security and meet customer's requirements. To detect and block east-west attacks from the Internet and tenant virtual networks, HUAWEI CLOUD deploys Intrusion Prevention Systems (IPSs) at the network borders, including but not limited to extranet borders, security zone borders, and customer space borders. IPS provides real-time traffic analysis and blocking capabilities to defend against attacks such as abnormal protocol attacks, violent attacks, port/vulnerability scanning, viruses/Trojan horses, and vulnerability-based attacks.

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
4.5	Malware protection	FIs shall implement malware one or more protection measures on every system to mitigate the risk of malware infection.	Customers need to install antivirus software on every system. To ensure the secure and stable running of the Huawei cloud platforms and networks, HUAWEI CLOUD takes a series of management measures, including vulnerability analysis and handling, log monitoring and event response, optimization of default security configuration of cloud products, security patch deployment, antivirus software deployment, and regular backup and test of system and device configuration files.

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
4.6	Multi-factor authentication	FIs shall perform multi-factor authentication on the following accounts: 1. All administrative accounts in respect of any operating system, database, application, security device, or network device in a critical system. A critical system refers to the system that may cause great damage to the bank operations or have great impact on the services provided for end users if it is faulty. 2. All accounts that can access customer information A concession is made for a period from 6 August 2020 to 5 February 2021 (both dates inclusive) on implementation of multi-factor authentication if: ● FIs identify all risks or potential risks posed by FIs' noncompliance to implement multi-factor authentication; and ● The appointed committee or members of the senior management agree with the risk assessment or are satisfied with the implemented controls being adequate to reduce the risks.	Customers need to perform multi-factor authentication on administrative accounts of critical systems and accounts that can access end user information. In exceptional cases, customers need to identify all risks or potential risks posed by FIs' noncompliance to implement multi-factor authentication and the appointed committee or members of the senior management agree with the risk assessment and are satisfied with the implemented controls being adequate to reduce the risks HUAWEI CLOUD provides IAM for customers to manage their cloud resource accounts. Customers can use IAM to verify user identities through passwords or multi-factor authentication. To meet customers' requirements, HUAWEI CLOUD has established a comprehensive O&M and operation account management mechanism. O&M engineers are required to provide employee identity accounts and use multi-factor authentication when accessing the HUAWEI CLOUD management network to centrally manage the system. In addition, the administrators of the HUAWEI CLOUD systems must pass the two-factor authentication before accessing the management plane through the jump

No.	Control Domain	Control Requirement	HUAWEI CLOUD Response
			server. Administrators' operations are logged and transferred to the centralized log audit system in a timely manner.

8 How HUAWEI CLOUD Meets 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* applies to FIs operating in Singapore. The Guidelines sets out minimum/ baseline control requirements that the outsourced service providers of FIs must adhere to, including auditing, inspections, entity level controls, general IT controls, and service controls. Outsourced service providers are also required to provide the *Outsourced Service Provider's Audit Report* (OSPAR) issued by third parties.

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

8.1 Audits and Inspections

The guidelineclearly 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	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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
II	Criteria for qualification external auditor	external auditor or decides to appoint a different external auditor 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.	computing products and services. In order to build up the 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.	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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
V	Reporting and handling of control failure / qualification of control objectives	If the auditor finds 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	HUAWEI CLOUD will provide 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		other competent independent parties.	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 subcontractors of outsourced service providers.	Customers should establish formal audit procedures and regularly audit their outsourcing suppliers. HUAWEI CLOUD will actively 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 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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		important and results of such monitoring should be provided to FIs.	financial customers from regulatory agencies.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
I. (e)	Information security policies	Information Security ("IS") policies and procedures are established, documented and reviewed at least every 12 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.	Customers should establish and regularly review formal information security policies and processes. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
II. (c)	Change managem ent	FIs should evaluate, approve, test, implement and review changes to applications, system software, and network components in a controlled manner. Establish development, 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.	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 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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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.

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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 provided to the customer.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 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	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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		technical support (EOS) date, assess the risks that may arise from continued use, and establish effective risk mitigation control measures where necessary.	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 providers is established and managed in accordance with the agreements and instructions of financial institutions.	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 *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 a hard-copy 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 determines data protection requirements, access rights and restrictions, and retention and destruction requirements.	To ensure customer security, HUAWEI CLOUD protects data in all stages of its lifecycle, from data creation, data storage, 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.*

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		subcontracting arrangements.	

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 a hard-copy 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)			

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

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

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 is reasonably and safely diverted so as to facilitate the separation of responsibilities.

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

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

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 target host.

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

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
13	Penetration testing	CSP penetration test reports can be used to ensure the security of 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.	Customers should conduct penetration testing of The CSP's environment. To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services. Together with partners, HUAWEI CLOUD has launched host intrusion detection, web application firewall, host vulnerability scanning, web page anti-tampering, and penetration test services, which enhance the security detection, correlation, and protection capabilities of HUAWEI CLOUD.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 record for disaster recovery/ business continuity.	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 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.

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

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

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4	Incident and problem management	Provide a reasonable level of security event 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.	Customers should establish formal incident and issue management procedures. 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.

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

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			resources meet the business needs of users.

Original No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 and operating system patches quickly.	Customers should establish formal asset management procedures, classify their assets, and define asset owners to quickly identify and fix vulnerabilities in assets. Customers can scan for external vulnerabilities and operating system vulnerabilities. They can detect asset content compliance, scan the configuration to compare it against the baseline, detect weak passwords, and perform other such functions through **HUAWEI CLOUD Vulnerability Scan Service (VSS)**. It can automatically discover the security risks of websites or servers exposed in the network, and help users to secure their business on the cloud from multiple dimensions. 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 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

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

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

10 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.

11 Change History

Released On	Version	Description
November 2019	1.0	This issue is the first official release.
March 2021	1.1	Added the compliance description of the MAS *Notice on Cyber Hygiene*.