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

Issue 2.0

Date 2024-12-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Background and Purpose of Publication

Following the recent wave of technological development, more and more FIs (Financial Institutions) are planning to transform their business by leveraging high-technology to reduce costs, improve operational efficiency and innovate. To regulate the application of Information Technology (IT) in the financial industry, the Bank of Thailand (BoT) and the Office of the Securities and Exchange Commission (OSEC) and the Office of Insurance Commission (OIC) published a series of regulatory requirements and guidelines, covering technology risk management, IT outsourcing management, and cloud computing implementation for FIs operating in Thailand.

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

1.2 Introduction of Applicable Financial Regulatory Requirements in Thailand

The Bank of Thailand (BoT)

- **No. FPG 8/2557 Regulations on Outsourcing of Financial Institutions**: For FIs that use outsourcing services, the BoT proposes relevant requirements for outsourcing management that FIs are required to comply with, and also provides risk management guidelines related to those outsourcing activities.
- **No. FPG 21/2562 Information Technology Risk Regulations of Financial Institutions**: Setting out IT risk management principles and implementation guidelines to assist FIs in establishing a sound and robust technology risk management framework.
- **No. Sor Nor Chor. 6/2561 Regulations on General Supervision of Undertaking Designated Payment Service Business**: Comprehensive regulatory regulations for payment service providers designated in Thailand, including governance, risk management, user protection, etc., have been developed, forming a clear regulatory framework.
- **No. Sor Nor Chor. 11/2561 Policies and Measures on Security of information Technology Systems**: Provide information technology system security policies and

standards for payment systems, designated payment systems and designated payment service providers in Thailand.

- **No.FPG.16/2563 Regulations on the Use of Services From Business Partners of Financial Institutions**: This regulation sets out regulatory requirements for FIs to select third parties or business partners to outsource some functions of financial services. The Bank of Thailand hereby issues regulations on the use of financial institutions' business partners' services to enable financial institutions to comply with them.
- **No. Sor Nor Chor. 1/2564: Regulations on the IT supervision of payment systems and services providers**: Provide for information security risk assessment of payment systems used by FIs.

The Office of the Securities and Exchange Commission (OSEC)

- **No. Sor Thor. 38/2565 Rules in Detail on Establishment of Information Technology System (2023)**: Setting out IT governance and information security management requirements regarding establishing information technology systems for intermediaries engaged in securities services.
- **No. Nor Por. 7/2565 Guidelines for Establishment of Information Technology System (2023)**: It is an interpretation of ***Rules in Detail on Establishment of Information Technology System***, and provides guidelines and best practices to meet the requirements related to the company's IT governance and information security management.
- **Cloud Computing Practice Guide**: Providing guidelines to FIs to understand the potential risks of cloud computing, and how to conduct risk management and implement security controls when using cloud computing services.

The Office of Insurance Commission (OIC)

- **B.E. 2563 (2020) OIC Guidelines for Governance and Management for information Technology Risk for Life Insurance Companies**: Standard for providing information technology risk supervision and management for Thai life insurance companies.
- **B.E. 2563 (2020) OIC Guidelines for Governance and Management for information Technology Risk for Non-Life Insurance Companies**: Standards for providing information technology risk supervision and management to non-life insurance companies in Thailand Standards for providing information technology risk supervision and management to non-life insurance companies in Thailand.

1.3 Definitions

- **HUAWEI CLOUD**

  HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, including Huawei Technologies (Thailand) Co., Ltd., and Sparkoo Technologies (Thailand) Co., Ltd., committed to providing stable, secure, reliable, and sustainable cloud services.

- **Customer**

  Registered users having a business relationship with HUAWEI CLOUD.

- **Outsourcing**

  Means contracting with a service provider to perform operations that are usually done partly or completely by FIs themselves.

- **Service provider**

Means other juristic person who enters into a contract to perform the functions which are normally done by financial institutions themselves, including any person who subcontract from the original service provider or from any subcontractor.

- **Cloud computing**

  Means a type of internet-based computing that provides shared computer processing resources and data on demand according to the definition by the National Institute of Standards and Technology (NIST) and/or definition by applicable Thai laws and regulations or the binding orders of the relevant Thailand government agencies.

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 obtained a number of international and industry security compliance certifications, ensuring the security and compliance of businesses deployed by customers.

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

Example of Huawei Cloud Partial Standard Certification：

Certification	Description
ISO27001	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO27017	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.
ISO27018	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.
TL 9000& ISO 9001	ISO 9001 defines a set of core standards for quality management systems (QMS). It can be used to certify that an organization has the ability to provide products that meet customer needs as well as applicable regulatory requirements.

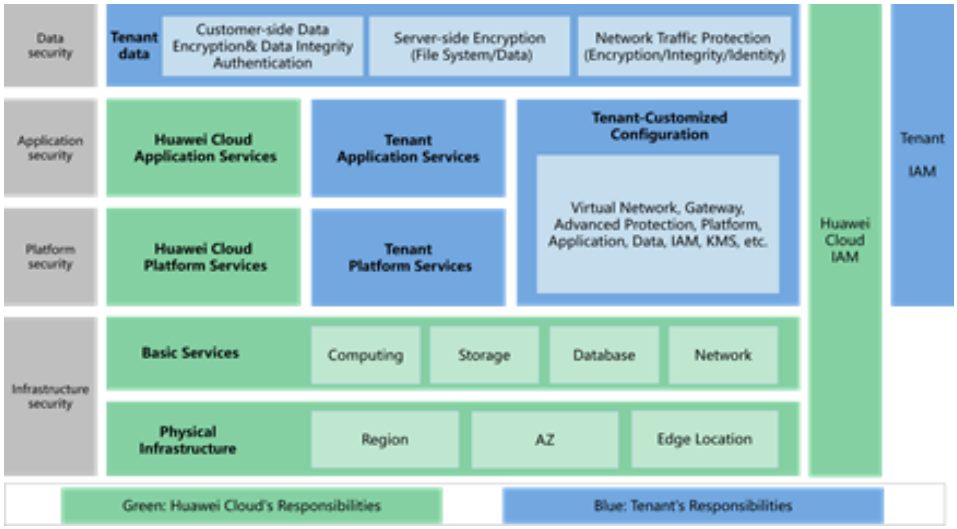
Certification	Description
	TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000. Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.
ISO 20000-1	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO22301	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
ISO27701	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
ISO29151	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.

Certification	Description
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.
ISO 27799	ISO/IEC 27799 provides guidelines on how organizations in the healthcare industry can better protect the confidentiality, integrity, traceability, and availability of personal health information. Huawei Cloud is the world's first cloud service provider to earn ISO/IEC 27799 certification. This certifies Huawei Cloud's deep understanding of intelligent applications for the healthcare industry, and its ability to protect the security of personal health information.
ISO 27034	ISO/IEC 27034 is the first ISO standard for secure programs and frameworks. It clearly defines risks in application systems and provides guidance to assist organizations in integrating security into their processes. ISO/IEC 27034 provides a way for organizations to verify their own product security and make security a competitive edge. This standard also outlines a compliance framework at the application layer for global cloud service providers, promoting the security of the R&D process, applications, and the cloud. Huawei Cloud is the world's first cloud service provider to obtain ISO/IEC 27034 certification. This marks a big step forward for Huawei Cloud governance and compliance.
SOC Audit Report	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.

3 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model



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

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

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

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

4 HUAWEI CLOUD Global Infrastructure

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

Regulations on Outsourcing of Financial Institutions: the BoT classifies outsourcing services according to their set of operations, licensing conditions for different types of outsourcing, and provides guidelines and requirements for FIs related to the management of their outsourcing activities. Those requirements cover the responsibilities of the board of directors, selection of service providers, consumer protection, business continuity management, contracts and agreements, and other domains, which provide the guidelines for the management of outsourcing by FIs.

When FIs are seeking to comply with the requirements provided in the *Regulations on Outsourcing of Financial Institutions*, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in *Regulations on Outsourcing of Financial Institutions*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

5.1 Selection of Service Providers

Clause 2 of Attachment 3 of *Regulations on Outsourcing of Financial Institutions* specifies that FIs must have service provider selection criteria. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Attachment 3 Clause 2	Selection of Service Providers	FIs must have appropriate service provider selection criteria prior to entering into a new contract or renewed contract, covering the following key issues. (1) Technical ability,	Customers should establish service provider selection criteria. **(1)Technical ability:** HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		expertise, and operating experiences, (2) Financial strength (3) Business reputation, records of complaints or litigation, (4) Organizational culture and service policy that is appropriate for FIs, (5) Ability to respond to new developments, (6) Concentration risk, and (7) Clear regulations on consideration of outsourcing to service providers related to the board and senior management	scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, HUAWEI CLOUD has created a new multi-computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. **(2)Financial strength:** HUAWEI CLOUD is Huawei's service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. According to the *Market Share: IT Services, worldwide 2019* study released by Gartner, HUAWEI CLOUD ranked sixth in the global IaaS market and is one of the top three within China market, with a fastest growth rate up to 222.2% in the world. **(3)Business reputation:** As always, HUAWEI CLOUD adheres to the customer-centric principle, making more and more customers choose HUAWEI CLOUD. HUAWEI CLOUD has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. **(4)Corporate culture and service policies suitable for FIs:** HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, laws and regulations, regulatory requirements in product, service planning and design phases. Huawei implements these in R&D, and design phases to meet

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and Huawei's comprehensive cloud services. **(5)Ability to respond to new developments:** Since its launch, HUAWEI CLOUD has insisted on technological innovation. It has released a series of leading new products and upgrades, covering many fields such as cloud security, DevOps, cloud container engine and micro service engine, service grid, computing, cloud storage, network, cloud disaster recovery, and so on. **(6)Risk management capability:** HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. **(7)Operational capability:** HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.

5.2 Consumer Protection

Attachment 3 Clause 3 of *Regulations on Outsourcing of Financial Institutions* states that "Financial institutions must always be aware that outsourcing is the only delegating services to the service providers. Financial institutions continue to be responsible to customers as if the financial institutions provide the services themselves. Therefore, financial institutions must ensure that the customers are treated properly." Being FIs' cloud service provider, HUAWEI CLOUD's responsibilities s are subject to the protection of FIs themselves. Clause 3 of Attachment 3 of *Regulations on Outsourcing of Financial Institutions* requires FIs to establish consumer protection mechanism. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Attachment 3 Clause 3(1)	Customer Data Confidentiality	Must ensure that the service providers are able to arrange a good system to maintain security and confidentiality of customer information and the financial institution information.	HUAWEI CLOUD strictly adheres to "not accessing customer data without permission" and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. HUAWEI CLOUD conforms to the data protection principles described in *the Personal Data Protection Act* (PDPA). At the same time, it will clearly stipulate the responsibility of HUAWEI CLOUD to customers in the case of a breach of confidentiality clauses in contracts signed with customers in the financial industry. In addition, HUAWEI CLOUD service products and components have planned and implemented isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature.
Attachment 3 Clause 3(2)	Problem and Incident Management	Must arrange to have an adequate system to handle customer complaints and problem solving by recording and monitoring customer complaints including the problem of	Customers should establish formal incident and problem management procedures. HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so customers can seek help with

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		customer information leakage, where FIs must specify appropriate guidelines to solve such problem.	methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager. To meet the requirement for fast response, HUAWEI CLOUD has developed a complete event management process. Events are prioritized and different processing time limits are defined according to the impact and scope of each event. HUAWEI CLOUD will respond to and resolve the event within a specified time limit according to the priority of the event, to minimize the impact of the event on cloud service customers.
Attachment 3 Clause 3(3)	Performance Monitoring and Capacity Planning	Must ensure that the service quality for customer does not deteriorate or the cost burden that normally incurs to FIs is put on customer.	Customers should establish performance monitoring and capacity planning mechanisms. *HUAWEI CLOUD Service Level Agreement* specifies the products/service level provided, including the commitment to service availability and compensation when failing to meet the agreed service level. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a standard capacity management and resource forecasting procedure to manage Huawei's cloud capacity as a whole and improve the availability of Huawei's cloud resources. HUAWEI CLOUD resource utilization is monitored daily. Input from all parties provides ongoing predictions for future resource requirements, and resource expansion schemes are formulated to meet these requirements. Business capacity and performance bottlenecks are analyzed and evaluated. When resources reach a preset threshold, a warning is issued, and further solutions are adopted to avoid the impact on the system performance of the tenant cloud service. Cloud Eye Service (CES) provides users

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			with a robust monitoring platform for Elastic Cloud Server (ECS), bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.
Attachment 3 Clause 3(5)	Customer Data Deletion	In case of contract termination or cancellation based on any reasons, FIs must ensure that customer's information is destroyed or is entirely removed from the service providers.	When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating to local data center. Upon the confirmation of the destruction of customer data by the customers, HUAWEI CLOUD clears the specified data and all the copies. Once customers agree the deletion, HUAWEI CLOUD deletes the index 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.

5.3 Business Continuity Management of Service Providers

Clause 4 of Attachment 3 of *Regulations on Outsourcing of Financial Institutions* requires FIs to implement business continuity management related to service providers. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Attachment 3 Clause	Business Impact Analysis	FIs must specify the significant level of the outsourced activity by	To provide continuous and stable cloud services to customers, HUAWEI CLOUD has established a set of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(1)	and Risk Assessment	assessing the risks and impacts that may incur if the services are disrupted.	complete business continuity management systems in accordance with *ISO 22301 - Business Continuity Management International* standards. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business.
Attachment 3 Clause 4(2)	Business Continuity Plan Development and Testing	FIs must require that the service providers have a business continuity plan especially for the case that significant activity or the activity with wide impact, as well as allocate adequate resources for such operation, applying the guidelines by the BoT on business continuity management (BCM) and business continuity plan (BCP) of FIs to the extent that is in consistent with the FIs' own business continuity. FIs must conduct a regular test on the business continuity plan with the key service providers, and must record the test results in writing to be reviewed by the BoT.	HUAWEI CLOUD follows ISO 22301 international standards for business continuity management and has established a complete set of business continuity management systems. Within this framework, business impact analysis and risk assessment are carried out regularly, business continuity plans and disaster recovery plans are formulated. As a supplier of cloud service customers, HUAWEI CLOUD will actively cooperate with customer-initiated test requirements and help customers test the effectiveness of their business continuity plans. HUAWEI CLOUD tests the business continuity plans and disaster recovery plans annually according to the requirements of the internal business continuity management system. All emergency response personnel, including reserve personnel, need to participate. The tests include desktop exercises, functional exercises and full-scale exercises, in which high-risk scenarios are emphasized. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After the completion of the test, relevant personnel write the test report and summarize any problems found during the test. If the test results show problems with the business continuity plan, recovery strategy or emergency plan, the relevant documents will be

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

5.4 Contracts and Agreements

Attachment 3 Clause 5 of *Regulations on Outsourcing of Financial Institutions* requires FIs to sign written contracts and agreements with service providers. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Attachment 3 Clause 5	Contracts and Agreements	FIs must enter into a written contract or agreement with the service providers, taking into account, at the minimum, the following key issues: (1) Detail of the service type, scope of responsibility, risk management, internal control process, security system for safeguarding information and assets of FIs; (2) Service level agreement to specify minimum standard of operation that the service providers must perform both under normal and abnormal situations; (3) Business continuity plan of the service providers to support the case where outsourced services are disrupted or unable to provide continuous services; (4) Process to monitor, audit, and evaluate performance of the service providers;	HUAWEI CLOUD provides online version of *HUAWEICLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		(6) Term of contract, terms and contract termination conditions, including the right of FIs to revise or extend the contract; (7) Scope of responsibility of the counter parties in case that a problem incurs such as service delay and mistake, as well as problem solving guidelines or compensation of loss (8) Information security, maintaining the confidentiality of customer information, FIs' information, and access right and information ownership, as well as data transmission, data maintenance, clear penalty in case that the breach of customer's and FIs' information. In this regard, the service providers should separate the data base of FIs' customers from that of the service providers as well as the service providers' other customers. (12) Compliance with the supervisory regulations (13) Assigning the right for the BoT, FIs, external auditors, or other government agencies to inspect operations, internal control process, as well as request relevant information from the service providers or	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		subcontractors (if any).	

5.5 Monitoring, Assessing, Auditing, and Controlling Risks from Outsourcing Activities

Clause 6 of Attachment 3 of *Regulations on Outsourcing of Financial Institutions* requires FIs to monitor, assess, audit, and control risks from outsourcing activities. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Attachment 3 Clause 6(2)(4)(5)	Control of Outsourcing Activities	(2) Arrange or have the service providers prepare an operating manual and relevant documents, as well as regularly updating them for the purpose of monitoring, evaluating, and risk management of FIs. (4)Arrange to have written documents on problematic or risk issues, loss data, as well as received orders from relevant authorities in conjunction with outsourcing services for review by the BoT. (5) Arrange to review the service provided regularly as deemed appropriate to the function group.	HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. In order to meet the compliance requirements of customers, HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system. In addition, HUAWEI CLOUD has a dedicated team to maintain the products descriptions and operating manuals regarding cloud services , and both of them are available in English and accessible on the international website. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. In addition, HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			provides 24/7 service support so customers can seek help with methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.

6 How HUAWEI CLOUD Meets the Requirements of BoT Information Technology Risk Regulations of Financial Institutions

In November 2019, the BoT released *Information Technology Risk Regulations of Financial Institutions*, providing principles of information technology risk management for FIs and implementation guidelines for information technology risk management and third party risk management.

When FIs are seeking to comply with the requirements of *Information Technology Risk Regulations of Financial Institutions*, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following materials summarize the compliance requirements related to cloud service providers in *Information Technology Risk Regulations of Financial Institutions*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.3.2(2)	Data Security	A FI must have information security controls for data transmitted through communication networks and data stored in IT systems and any storage media. And, to ensure data confidentiality, data must be appropriately classified, kept and disposed depending on its classification, and encrypted by a reliable and generally accepted encryption technique at international standard (cryptography).	Customers should consider protecting all media that stores information, both paper and electronic. When customers use encryption to protect data, they should consider using industry-approved encryption algorithms and key management mechanisms. HUAWEI CLOUD has developed a sound media management process for storage media that stores customer content data in the financial industry to ensure the security of the data stored in the media. 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 in agreement with the customer to erase the stored customer data. Specific practice is: Once

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. Currently, services including Elastic Volume Service (EVS),Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. 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. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to meet users' data security compliance requirements. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with customers' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys.
5.3.2(3)	Access Control	A FI must have the control of access and the right of audit to its operating systems and databases, as there must be the	Customers should establish a mechanism for authentication and access control management of the information system, and restrict and supervise the behavior of the access system.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		management of access rights and authentication. The access rights must be given depending on the need to access any particular system and risk level in order to prevent the access and revision to systems or data by unauthorized persons.	Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM). Except for the support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. In addition, HUAWEI CLOUD's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			responsibilities in different positions are limited to access the equipment under their role.
5.3.2(4)	Physical and Environmental Security	A FI must have security controls for its data centers, IT workplaces, as well as the areas of critical IT systems. There must also be a protection system and maintenance process for computer hardware and facility system connected to IT systems in order to prevent possible attacks or damage from natural disasters and ensure that they can continuously support the business operations.	Customers should develop and implement physical and environmental security management processes. HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standard of *TIA-942 Telecommunications Infrastructure Standard for Data Centers*. HUAWEI CLOUD data centers are located on suitable physical sites, as determined from solid site surveys. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The HUAWEI CLOUD O&M team carries out risk assessment to enforce stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers. See section 5.1 Physical and Environmental Security of *HUAWEI CLOUD Security White Paper* for more information.
5.3.2(5)	Communications Security	A FI must have security controls for its communication systems so that the systems and data transmitted through	Customers should establish a network security management system to ensure that all information located and processed within its network are protected. HUAWEI CLOUD ensures that

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		them are secure and protected from any possible attacks or threats.	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. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent.
5.3.2(6)	Operations Security	A FI must have security controls for its IT operations so that the IT operations are secure, which must cover, but not limited to, the following: (6.1) Capacity management for IT systems and facility systems, such as conducting an	**1. Capacity management:** Customers pass through HUAWEI CLOUD's Cloud Eye Service (CES) Cloud Eye Service (CES) which provides three-dimensional monitoring of elastic 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. These metrics allow users to set alert rules and notification policies to keep abreast of the health and performance of instance

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		assessment of the future demand for IT resources so that the IT resources are properly managed, as they can sufficiently support the business operations, while the FIs can manage IT resources to deal with its future needs; (6.2) Security controls for the severs and user devices (endpoint devices), such as installing anti-virus or anti-malware software or cyber attack in order to prevent data leakage or unauthorized access; (6.3) Data backup – data must be backed up using an appropriate approach within an appropriate timeframe , such as on a daily basis so that the backup data is ready to use whenever the original data is unavailable or damaged; (6.4) Keeping of logs of the servers and important networking hardware, such as keeping and reviewing access logs and activity logs in order to monitor and inspect the access and the use of the system or data; (6.5) Security monitoring – there must be a process or tools for monitoring suspicious incidents or threats that may affect critical IT systems, such as installing a system for monitoring	resources for each service. HUAWEI CLOUD has also developed a complete performance and capacity management process through early identification of resource requirements, and overall management of platform resource capacity and equipment inventory, HUAWEI CLOUD can continuously optimize resource utilization and resource availability levels, and ultimately ensure that cloud resources meet the business needs of users. **2. Host security management:** Customers can use the HUAWEI CLOUD Host Security Service (HSS) Host Security Service (HSS) to protect host security. HSS provides asset management, vulnerability management, baseline check, and intrusion detection functions to help enterprises better manage host security risks, detect and prevent hacker intrusion in real time, and meet graded security protection compliance requirements. **3. Backup management:** HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS)Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS)Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also back up data through HUAWEI CLOUD's data backup archiving service to ensure that data will not be lost in the event of a disaster. **4. Log and monitoring management:** HUAWEI CLOUD's Trace Service (CTS) provides operating records of cloud service resources for users to query, for auditing and backtrack use. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and analyzing cyber threats so that the FIs can promptly detect, prevent and handle suspicious incidents or threats; (6.6) Management of system vulnerability according to risk level – so that the vulnerabilities can be detected and the FIs can promptly take further actions to prevent possible threats; a vulnerability assessment for critical IT systems must be conducted at least once a year or when there is any significant change of technical standard; (6.7) Penetration test, which may be conducted by an independent internal or external expert; the test must cover internet-facing systems and be conducted at least once a year or when there is any significant change in order to detect the vulnerabilities and that the FIs can promptly make improvements to prevent possible threats; (6.8) Change management – there must be a secure and sufficient process for managing and controlling the changes, which may be in form of, such as, system deployment, system configuration, patch installment, in order to ensure that the change takes place	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; 1. 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; 2. In the storage phase, it adopts multiple backups according to Huawei's network security specifications and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance. **5. Vulnerability and patch management:** The Huawei Product Security Incident Response Team (PSIRT) became an official member of the Forum of Incident Response and Security Teams (FIRST) in 2010, through which Huawei PSIRT and the other 471 members can share incident response best practices and other security information. Huawei PSIRT has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD's self-service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		correctly and completely reaches the specified objectives and the unauthorized change is prevented; (6.9) System configuration management – there must be a control process for the configuration of production systems, and the configuration must be regularly reviewed in order to prevent operational errors; (6.10) Patch management – there must be a control process for the installment of patch on production systems in order to promptly install the important security patch.	vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations. 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. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on tenant services. In addition, HUAWEI CLOUD Image Management Service (IMS) provides simple and convenient self-service management functions for images. Tenants can manage their images through the IMS API or the management console. HUAWEI CLOUD staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. **6. Penetration testing:** 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. **7. Change management:** To meet customer compliance requirements, HUAWEI CLOUD has formulated a standardized change management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			process. Any change to the environment will take place only by orderly management process. After all change requests are generated, they are submitted to the HUAWEI CLOUD Change Committee by the change manager team with change classification assigned. After the committee has reviewed and approved the requests, the planned changes can be implemented on the production network. Before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. **8. Configuration management:** 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.
5.3.2(7)	System Acquisition, Development and Maintenance	(7.1) **System acquisition:** A FI must set out clear and appropriate criteria for the selection of system and service provider, which should cover, for example, the credibility of system or service provider, certification (according to international	Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		standards or generally accepted IT standards), system security, system support and maintenance, to ensure that the system and service provider can respond to business needs of the FIs. Other key concerns may include the flexibility in the replacement of service provider, technological changes, and future changes in business strategies of the FIs. (7.2) **System development**: A FI must carry out the design, development and testing of system to ensure that the system is accurate, secure, reliable, ready to use, and is flexible enough to accommodate any changes in the future.	analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified, the design engineer will formulate mitigation measures according to the reduction library and the safety design library and complete the corresponding safety design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the safety of products and services. HUAWEI CLOUD strictly complies with the security coding specifications of various programming languages issued by Huawei. Static code analysis tools are used for routine checks, and the resulting data is entered in the cloud service tool chain to evaluate the quality of coding. Before all cloud services are released, static code analysis alarms must be cleared to effectively reduce the security issues related to coding when online. HUAWEI CLOUD takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services to ensure that the released cloud services meet security requirements. Testing is conducted in a test environment, isolated from the production environment, and avoids the use of production data for testing. If production data is used for testing, it must be desensitized, and data cleaning is required after use.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.3.2(8)	IT Incident and Problem Management	A FI must properly and promptly manage IT incidents and problems, where the incidents and problems must be recorded, analyzed, and reported, together with the resolutions, to the board of directors, designated committee or senior managements in a timely manner. In addition, the FIs must figure out the root causes of those problems in order to resolve the actual problems and prevent a recurrence of the incidents.	HUAWEI CLOUD, as a CSP, is responsible for the event and change management of its infrastructure and various cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a complete event and management process to regularly review and update it. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source.
5.3.2(9)	IT Business Continuity Plan	(9.1) A FI must set up a working group or appoint a particular unit to be responsible for preparing an IT business continuity plan, which must be in written and in line with the specified policy. (9.3) An IT business continuity plan must be practical as it can effectively be used to mitigate losses, and must be in accordance with the Policy Statement of the BoT Re: Business Continuity Management (BCM) and Business Continuity Planning (BCP) of FIs. The plan must specify the recovery time objective (RTO) and	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 provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		recovery point objective (RPO), which will depend on the materiality of system, as well as the maximum tolerance period of disruption (MTPD) to ensure the continuity of business operations of the FIs and that the plan can deal with the incidents that may lead to a disruption or damage to the system, such as cyber threats, natural disasters. The plan will also ensure that the FIs can rapidly recover the system and recover to its normal operations. (9.5) An IT business continuity plan must be reviewed and tested at least once a year or when there is any significant change. (9.6) A FI must set up a disaster recovery site that is ready to operate whenever the primary site encounters a disruption. The disaster recovery site should be remote from the primary site to ensure that they do not share the same disruptions or have been affected from the same causes at the same time, such as power outage, natural disasters.	process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. As a supplier of cloud service customers, HUAWEI CLOUD will actively cooperate with customer-initiated test requirements and help customers test the effectiveness of their business continuity plans. HUAWEI CLOUD tests the business continuity plans and disaster recovery plans annually according to the requirements of the internal business continuity management system. All emergency response personnel, including reserve personnel, need to participate. The tests include desktop exercises, functional exercises and full-scale exercises, in which high-risk scenarios are emphasized. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After the completion of the test, relevant personnel write the test report and summarize any problems found during the test. If the test results show problems with the business continuity plan, recovery strategy or emergency plan, the documents will be updated. In order to meet the compliance requirements of customers, HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when getting the notification of personnel changes. Multiple copies of documents such as the business continuity plan, emergency

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			response plan and disaster recovery operation manual are stored both electronically and in paper form and are distributed to relevant management and other key personnel. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.
5.3.2(10)	Third Party Management	(10.1) Define clearly and in writing the roles and responsibilities between FIs and third parties, and stipulate the conditions under which the BoT has the right to inspect the operation of third parties; (10.2) Monitor and manage risks arising from connecting with or obtaining information from third parties when using the services; (10.3) Ensure that the information security of the third party conforms to the information technology security standards of FIs and the recognized international standards	HUAWEI CLOUD provides online version of *HUAWEI CLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. As the case may be, the auditing and supervision rights of customers and regulatory authorities will be stipulated in the agreement signed with the customer. HUAWEI CLOUD provides online version of *HUAWEICLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. As the case may be, the auditing and supervision rights of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		of network security; (10.4) Respond in time to possible events and events that have a significant impact on FIs to ensure that they can continue to conduct business.	customers and regulatory authorities will be stipulated in the agreement signed with the customer. If a FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible personnel to actively cooperate with the audit. 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. In addition, 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.

7 How HUAWEI CLOUD Meets the Requirements of BoT Regulations on General Supervision of Undertaking Designated Payment Service Business

7.1 General regulations for supervision

Business providers of designated payment services shall appropriately manage risks associated with the undertaking of designated payment service business to be in line with business model. The risk management process must be able to identify, assess, monitor, control or mitigate the potential risks; and at least shall comply with the following regulations:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.2.3(1)	Risk Management Policy	(1) Establish clear risk management policy for payment service in writing to be in line with business model, size, volume of transaction and complexity of the business, which must be approved by the board of directors or the assigned committee. It should incorporate the guidelines, practices, authorized persons for risk management and assessment, as well as report the outcome to the board of directors or the committee or the authorized management within appropriate timely manner.	Customers should establish a written risk management policy that is appropriate to the business model, size, volume and complexity of the business. The risk management policy needs to be approved by the board or committee, and the customer needs to report to the board or management on risk management on a regular basis. HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company.
4.2.3(2)	Business Continuity Management	(2) Establish Business Continuity Management (BCM) and Business Continuity Plan (BCP) to support any problems or incidents that may occur, and to be consistent with the type and complexity of the businesses in order to minimize the impact.	Customers should establish business continuity management policies and corresponding business continuity plans and procedures. HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
4.2.3(5)	Outsourcing management	(5) Outsourcing In the case that business providers of designated payment services use services provided by other service providers or third parties (outsourcing) for the operation on behalf of themselves in the IT system functions, including functions that have a significant impact on the business, business providers of designated payment services are still responsible for service users in providing the services with continuity, security, reliability and for any potential damages as if the services are provided by business providers	When IT system functions involving payment services are outsourced, customers need to establish a third-party review and evaluation process, sign an outsourcing agreement, develop a BCP and DRP covering outsourcing activities, and evaluate cross-outsourced risks and cross-border data compliance when using cross-outsourced services. HUAWEI CLOUD provides online version of *HUAWEICLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		themselves. Business providers of designated payment services shall take actions as follows: (5.1) Have in place an appropriate risk management process including selection, monitoring, evaluation and examination of the services provided by other service providers or third parties; and assess risks arising from outsourcing activities on a regular basis. In this regard, risk assessment should cover risks related to protection of confidentiality and data privacy as well as an impact on the critical systems of business providers of designated payment services. (5.2) Have in place an outsourcing agreement which indicates the rights of internal auditor, external auditor and the BoT to perform an audit of the operations and internal control of other service providers or third parties in the parts relating to the undertaking of designated payment service business. (5.3) Have in place a Business Continuity Plan (BCP) or a Disaster Recovery Plan (DRP) that cover the outsourcing activities, including the testing and reviews of the implementation of the plans on a regular basis in order to ensure that the plan can be practically implemented. (5.4) In case of selecting service provided by other service providers or third parties from overseas especially for data storage, data processing or any other operations relating to data, business providers of designated payment services must assess potential risks that may arise from such offshore outsourcing activities such as	provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. As the case may be, the auditing and supervision rights of customers and regulatory authorities will be stipulated in the agreement signed with the customer. HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. HUAWEI CLOUD provides services for customers through global resources. Therefore, the customer's account data may be transferred to or accessed by the countries or regions where HUAWEI CLOUD affiliates and HUAWEI CLOUD partners are located. In this case, HUAWEI CLOUD will ensure that the transfer complies with applicable legal requirements

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the risk of not being able to access to data due to disruption or blocking of the communications networks or the international communications system (Information Access Risk) and the legal risk related to the compliance with foreign countries' regulations (Cross-border Compliance), as well as prepare the supporting plan to manage potential risks.	and passes strict internal review. For example, HUAWEI CLOUD will sign a data transfer agreement that can fully protect personal data, or inform the customer of the necessity and potential risks of cross-border data transfer, and obtain the customer's explicit consent.

8 How HUAWEI CLOUD Meets the Requirements of BoT Policies and Measures on Security of information Technology Systems

8.1 Appendix: Guidelines on Security of IT Systems relating to the Payment Systems

<Policies and Measures on Security of information Technology Systems> released by BoT mainly provides security construction guidelines for IT systems of payment institutions through its Appendix <Guidelines on Security of IT Systems relating to the Payment Systems>.

8.1.1 Access Control

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
1.1	Separation of duties	The service providers or the business providers shall assign	Customers should: (1) Clarify the division of responsibilities and responsibilities of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		duties and responsibilities to staff or units accountable for security of information technology systems as well as create awareness, provide knowledge and train the staff in the organization including create the disciplinary procedures for punishment in case where there is violation or breach of security rules & regulations.	each domain of information technology system security to ensure mutual checks and balances to prevent possible operation risks. (2) Provide training, education and awareness-raising, including regular communication with personnel within the organization, to keep staff abreast of developments in technology and new threats. (3) Establish disciplinary procedures to punish personnel who violate or violate policies or regulations related to information technology system security. Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Except for the support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			ensure that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different responsibilities in different positions are limited to access the equipment under their role.
1.2	Access Control for Information Technology Systems	The service providers or the business providers shall establish written procedures for controlling and limiting the access rights to the information technology systems relating to service and information as needed, in order to prevent the hacking or access into the system of the unauthorized people from both inside and outside the organization.	Customers should establish formal access control management policies and procedures and establish appropriate access control over the critical information systems for which the Organization provides services. You can use Identity and Access Management (IAM) to manage user accounts that use cloud resources. If the tenant has a secure and reliable external identity authentication service provider, you can map the federated authentication external user of IAM to a temporary user of HUAWEI CLOUD and access the tenant's HUAWEI CLOUD resources. In addition, when HUAWEI CLOUD O&M personnel access the HUAWEI CLOUD management network to manage the system in a centralized manner, they need to use unique employee accounts. Strong password security policies are configured for user accounts, and passwords are changed periodically to prevent brute force password cracking.
1.3	Identity Authentication and Prevention of Denial of Responsibility (repudiation)	The service providers or the business providers shall provide identification, authentication or verification of user identity by using appropriate technology to be associated with the risk level of each business type e.g. the use of password, personal identification number, token or smart	Customers should use passwords, personal identification numbers, tokens or smart cards, biometrics or public key infrastructures to identify, authenticate or verify the user's identity, record the behavior of each account, record details of the use of information technology systems, and retain them as evidence of review in the event of a problem. When HUAWEI CLOUD O&M personnel access the HUAWEI CLOUD management network to manage the system in a centralized manner, they need to use a unique and identifiable

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		card, biometric characteristics or public key infrastructure in order to prevent denial of liability in case of dispute.	employee account. Strong password security policies are configured for user accounts, and passwords are periodically changed to prevent brute force password cracking. HUAWEI CLOUD also uses two-factor authentication, such as USB key and Smart Card, to authenticate the identity of cloud personnel. Employee accounts are used to log in to the VPN and bastion host to implement in-depth user login audit. In addition, HUAWEI CLOUD Cloud Trace Service (CTS) collects, stores, and queries operation records of various cloud resources. It can be used in common scenarios such as security analysis, compliance audit, resource tracing, and fault locating.

8.1.2 Information Confidentiality and System Integrity

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.1	Information Confidentiality	The service providers or the business providers shall establish the appropriate steps and procedures in transmitting, processing and storing information in order to preserve confidentiality and accuracy of information.	Customers should determine the confidentiality level and access rights of the information based on the importance level, and establish procedures for reliable and secure transmission, processing, and storage, use, and destruction of the Confidential Information based on the importance level. HUAWEI CLOUD evaluates data security levels based on data confidentiality, integrity, availability, and compliance, and classifies data from severe to slight impacts caused by data damage and leakage. During the design and R&D phase, HUAWEI CLOUD formulates a data flow diagram to display the life cycle of various data in the service and operations performed by Huawei, and specify the operation purpose. For services involving personal data processing in each domain of HUAWEI CLOUD, the business owner regularly sorts out the personal data list involved in the service, and reviews and updates

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			the list every year. HUAWEI CLOUD has established data security management requirements and processes, specified the data owner of HUAWEI CLOUD data and tenant data, determined data security levels, and specified data use, security, and privacy protection requirements. HUAWEI CLOUD implements data protection measures and uses proper encryption technologies, recognized security protocols, secure encryption channels, or data encryption on transmission channels.
2.2	Development of systems, Change control management, Improvement of information technology systems or data processing equipment	The service providers or the business providers shall establish systematic procedures and internal control for developing and controlling over changes or improvement of information technology systems to reduce the risks of failure or malfunction of service systems.	Customers should implement changes to IT systems in accordance with Change Management and Systems Development guidelines. At the same time, customers should always update operating procedures, backup systems, and business continuity plans in response to any IT system changes. In addition, such changes should be communicated to the relevant personnel for confirmation so that the work can be performed correctly. To meet customers' compliance requirements, HUAWEI CLOUD has developed a standard change management process. Changes to each element of the production environment must be managed through orderly activities. After all change applications are generated, the change manager determines the change level and submits them to the HUAWEI CLOUD Change Committee. The changes can be implemented on the live network as planned only after they are approved. All changes must be fully verified in production-like environment tests, gray release, and blue-green deployment before being applied for to ensure that the change committee clearly understands the change actions, duration, rollback actions if the change fails, and all possible impacts. In addition, HUAWEI CLOUD formulates fine-grained change operation regulations to guide the implementation, tracking, and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			verification of the entire change, ensuring that the change achieves the expected purpose. In addition, HUAWEI CLOUD has developed a standard emergency change management process. If the emergency change affects the user, the system will communicate with the user in advance through announcements, emails, telephone calls, and meetings within the specified time limit. If an emergency change does not meet the specified notification time limit, the change will be escalated to HUAWEI CLOUD executives and announced to users in a timely manner after the change is implemented. All changes are recorded. The old program version and data are retained before the change is implemented. During the change process, the change is smooth through two-person operation mechanism to minimize the impact on the production environment. After the change is implemented, dedicated personnel are assigned to verify the change to ensure that the change achieves the expected purpose.
2.3	Management of network systems relating to service	The service providers or the business providers shall establish the preventive measures for the unauthorized access to the network system of services.	Customers should establish a network communication security management mechanism to ensure that the information and information processing facilities on the network are protected. HUAWEI CLOUD ensures the secure development, configuration, and deployment of various cloud technologies, and is responsible for the O&M security of provided cloud services. Therefore, HUAWEI CLOUD initially considers the network architecture design and device selection and configuration. It adopts various multi-layer security isolation, access control, and border protection technologies for physical and virtual networks, and strictly implements corresponding management and control measures to ensure HUAWEI CLOUD security. You can use the **Virtual Private Cloud (VPC)** and **Elastic Load Balance (ELB)** services provided by HUAWEI

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			CLOUD to implement network isolation and load balancing between different regions. A VPC can construct a private network environment for tenants, implementing complete Layer 3 network isolation between tenants. Tenants can fully control their own virtual network construction and configuration. By configuring network ACLs and security group rules, tenants can strictly control the network traffic entering and leaving subnets and VMs. This feature meets tenants' fine-grained network isolation requirements.

8.1.3 System Availability

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.1	Risk assessment and management of service system	The service providers or the business providers shall ensure the appropriate risk assessment methodology of service system, determine criteria for risk appetite and risk tolerance and procedures to manage the potential risks. In this regard, the service providers or the business providers shall regularly conduct the risk review in associated with technology development and current situations.	Customers should establish an appropriate risk management system for the business, develop a risk assessment methodology, and confirm the organization's risk appetite and risk tolerance standards and the means to eliminate/manage potential risks. HUAWEI CLOUD inherits Huawei's risk management capabilities and establishes a risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD effectively controls risks in complex internal and external environments and huge uncertain markets, strives to balance performance growth and risks, and continuously manages internal and external risks. Ensure the sustainable and healthy development of the company.
3.2	Monitor and detect abnormalities or vulnerabilities of the information	The service providers or the business providers shall monitor and detect abnormalities and also follow the news about vulnerability of various systems used in service in order to evaluate risks and determine	Customers should monitor and detect abnormal transactions and threats, evaluate system vulnerabilities, and develop measures to resolve or close system vulnerabilities. Penetration tests can be performed on high-risk systems to verify the effectiveness of security technologies. HUAWEI CLOUD has a centralized and complete log big data analysis system.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	technology systems	measures for risk mitigation.	The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. The logs contain resource IDs. (e.g. source IP, host ID, user ID, etc.) , event type, date and time, and ID of the affected data/component/resource. (e.g. destination IP address, host ID, service ID, etc.) 2. Success or failure information to ensure that cyber security incident backtracking and compliance are supported. HUAWEI CLOUD organizes internal and third-party evaluation organizations to scan all systems, applications, and networks of HUAWEI CLOUD every quarter, and hires external third parties to perform penetration tests on HUAWEI CLOUD applications and networks every six months. HUAWEI CLOUD will evaluate and analyze the vulnerabilities found in the penetration test, develop and implement the vulnerability fixing solution or workaround, and verify the solution after the vulnerability is fixed. If the vulnerability is found, continue to revise the vulnerability fixing solution. If the vulnerability passes the verification, follow the HUAWEI CLOUD change management process. Develop a vulnerability fixing plan based on the vulnerability SLA requirements, implement the vulnerability fixing or workaround, and report the fixing result to the management.
3.3	Resolution, Incident response, recording and reporting in case where the damages occur to the	The service providers or the business providers shall monitor, record, and report the incidents of security breach via the defined reporting channels as soon as possible. Moreover, the lesson learnt from the past experiences shall be taken into account for	Customers should establish a comprehensive security vulnerability and event management mechanism to detect, record, and report security vulnerabilities and events in a timely manner. HUAWEI CLOUD has developed a security event management mechanism and continuously optimizes the mechanism. The security incident response process clearly defines the roles and responsibilities responsible for each

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	information technology system.	the advance preparation of necessary preventive measures.	activity in the incident response process. HUAWEI CLOUD Big Data Analytics can quickly collect, process, and analyze massive logs in real time. It can interconnect with third-party security information and event management (SIEM) systems, such as ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. The system continuously monitors and analyzes security events in real time to detect security events in a timely manner. In addition, HUAWEI CLOUD has a 7 x 24 professional security incident response team and a corresponding security expert resource pool to handle security incidents. HUAWEI CLOUD defines security event grading and escalation principles, levels security events based on the impact of security events on customers' services, and initiates the customer notification process based on the security event notification mechanism to notify customers of the events. When a serious security incident occurs and has or may have serious impact on a large number of customers, HUAWEI CLOUD can notify customers of the incident information through bulletins as soon as possible. Include at least the description, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer. After the incident is resolved, an incident report will be provided to the customer on a case-by-case basis.
3.4	Information backup	The service providers or the business providers must have information backup and it must be regularly validated in order to preserve its accuracy, completion and availability of the service.	Customers should establish an information backup mechanism to ensure the availability and accuracy of backups through multiple backups or remote backups, and periodically verify the integrity of backups of information systems. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			in different scenarios. Customers use functions such as version control function of **Object Storage Service (OBS)**, **Volume Backup Service (VBS)** and **Cloud Server Backup Service (CSBS)** to back up documents, disks, and servers on the cloud. They can also use Huawei cloud backup and archiving solution. Back up on-premises data and archive it to HUAWEI CLOUD to prevent data loss in the event of a disaster. In addition, customers can rely on the multi-region and multi-AZs architecture of Huawei cloud data center clusters to implement disaster recovery and backup for their service systems. Data centers are deployed in different regions around the world according to rules. Customers can use two sites to serve as disaster recovery centers for each other. If one site is faulty, the system automatically transfers customer applications and data away from affected areas based on compliance policies, ensuring service continuity. HUAWEI CLOUD also deploys a global load balancing scheduling center. Customers' applications are deployed in N+1 DCs. Even if one DC fails, traffic can be balanced to other DCs.
3.5	Development of business continuity plan or emergency plan of IT systems	The service providers or the business providers shall develop the business continuity plan for service of the highly important payment systems, the designated payment systems or the designated payment services, as the case may be, and implement the plan to ensure the service can proceed within the defined timeline after the incident of service suspension occurred.	Customers should establish its own business continuity mechanism and formulate RTO and RPO indicators to ensure the continuity of key services. If a financial institution needs HUAWEI CLOUD to participate in its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the IS022301 certification. HUAWEI CLOUD conducts business continuity publicize and training in the organization every year, and regularly conducts emergency drills and tests to continuously optimize the emergency

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			response mechanism. Based on the requirements of the system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery level of key services. In the process of identifying critical services, the impact of service interruption on customers is an important criterion for determining critical services. To meet customers' compliance requirements, HUAWEI CLOUD formulates recovery policies for key services that support continuous operation of cloud services based on the requirements of the internal business continuity management system.

9 How HUAWEI CLOUD Meets the Requirements of BoT Regulations on the Use of Services from Business Partners of FIs

The BoT issued the <Regulations on the Use of Services from Business Partners of FIs> on December 23, 2020, which sets out regulatory requirements for financial institutions to select third parties or business partners to outsource some functions of financial services. The Bank of Thailand hereby issues the Regulations on the Use of Services of Business Partners of Financial Institutions. To enable financial institutions to comply.

When FIs comply with the <Regulations on the Use of Services from Business Partners of FIs>, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following section summarizes the control requirements related to cloud service providers in the <Regulations on the Use of Services from Business Partners of FIs> and describes how HUAWEI CLOUD, as a cloud service provider, helps financial institutions meet these control requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.2.1	Strategic function commitment	Financial institutions can use the services from business partners, both juristic persons and natural persons, that have in place appropriate guidelines on risk management and customer protection. However, strategic functions must be carried by financial institutions themselves.	FIs may use services provided by outsourced service providers, but should assume the strategic policy functions of their own organization HUAWEI CLOUD shall provide guidelines for financial institution customers on risk management and customer protection. HUAWEI CLOUD sets risk management objectives in compliance with the cost-effectiveness principle, formulates management mechanisms and detailed operation rules for HUAWEI CLOUD risk assessment, risk ceiling, and risk handling, comprehensively assesses risks in the business domain every year, specifies risk contact persons or risk handling owners for identified risks, and formulates risk handling solutions. Different levels of risk specify disposal requirements for different periods of time. HUAWEI CLOUD adheres to the bottom line of "do not touch data" and clearly states in the user agreement that it will not access or use users' content, except to provide necessary services for users, comply with laws and regulations or binding orders of government agencies, and comply with the data protection principles specified in Thailand's Personal Data Protection Law. In addition, the contracts signed with customers in the financial industry will specify HUAWEI CLOUD's responsibilities for customers in the event of breach of confidentiality clauses. In addition, isolation mechanisms are planned and implemented for HUAWEI CLOUD service products and components from the beginning of design to prevent unauthorized access and tampering between customers and reduce data leakage risks. Take data storage as an example. HUAWEI CLOUD block storage, object storage, and file storage services take customer data isolation as an important feature. As an outsourcing service provider of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			financial institutions, HUAWEI CLOUD presents its best practices on risk management and customer protection in white papers or compliance documents. Customers can visit the Trust Center on their official website to view related best practices.
5.3.1	General scope and conditions for the use of services by business partners	General scope and condition of using services from business partners (1) Financial institutions can use services from business partners in non-strategic functions, taking into account efficiency enhancement for business operation, enterprise risk management, cost, and business benefits of financial institutions in Thailand as the main purpose. (2) Financial institutions must perform strategic functions by themselves (principles and examples in attachment 1). In the case that financial institutions find it necessary to use service on strategic functions from business partners within the same business group, financial institutions shall apply for approval from the Bank of Thailand on a case-by-case basis. (3) Financial institutions can use services from business partners, both juristic persons and natural persons as well as both	FIs may use outsourced services for their own non-strategic functions, and should seek approval from Bank of Thailand if they find it necessary to use services for strategic functions of business partners within the same business group. FIs can use local or overseas outsourcing services, where financial companies and credit institutions can only use services provided by domestic outsourcers. Overseas branches of commercial banks registered in Thailand should comply with local regulatory requirements for outsourcing services and ensure the safety of customers. HUAWEI CLOUD adheres to the bottom line of "do not touch data" and clearly states in the user agreement that it will not access or use users' content, except to provide necessary services for users, comply with laws and regulations or binding orders of government agencies, and comply with the data protection principles specified in Thailand's Personal Data Protection Law. In addition, the contracts signed with customers in the financial industry will specify HUAWEI CLOUD's responsibilities for customers in the event of breach of confidentiality clauses. In addition, isolation mechanisms are planned and implemented for HUAWEI CLOUD service products and components from the beginning of design to prevent unauthorized access and tampering between customers and reduce data leakage risks. Take data storage as an example. HUAWEI CLOUD block storage, object storage, and file storage services take customer data isolation as an important feature.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		locally and overseas. (4) Finance companies and credit fonciers companies cannot appoint banking agents but can use services from outsourcers within the country. (5) Overseas branches of commercial banks registered in Thailand shall comply with regulations on scope and condition of using service from business partners and customer protection issued by regulators in the countries in which such branch is located.	
5.3.3	Risk Management	The use of business partners may cause risks to arise upon financial institutions such as reputational risks, operational risks, information technology risks from system connection with business partners, and business continuity risks when there is business partner's service disruption. Financial institutions must have risk management guideline to manage the use of business partners, as follow. (1) Financial institutions must establish guideline on the use of services from business partners, at least covering the scope of service to be used from business partners, level of significant risk or impact on customers	FIs must establish risk management guidelines or policies related to outsourcing services or the use of vendors to manage risks including information technology risks and business continuity risks in the event of a business partner's service interruption; FIs need to establish guidelines and policies for the use of outsourcing suppliers or outsourcing services, covering the scope of outsourcing services and risk impact analysis, and review the guidelines annually. When using outsourcing services, FIs shall ensure their customers' data security, complaint and service rights protection, business continuity of outsourcing services, and risk management system review of outsourcing service providers. FIs are required to review and manage the compliance of outsourced service providers, including data privacy laws, anti-money laundering laws, foreign exchange control laws and notices from the Bank of Thailand on market conduct. HUAWEI CLOUD uses indicators such as RPO, RTO, and DR success rate to evaluate the achievement of DR

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		at large, and it should be reviewed annually or when there are significant changes. (2) Financial institutions are required to ensure that business partners provide service to customers like they are conducted by financial institutions themselves, keeping the following 3 important principles; 1) appropriate protection of customers' minimum rights especially on security of data, handling of complaints and service problems, 2) business continuity and 3) management system of risks from using business partner's service that is appropriate to significant risk and impact level, covering related risks especially reputational risks, operational risks and information technology risks, where business partners selection process, and business partner risk management cover key issues (details in attachment 3-6). (3) Financial institutions must ensure that business partners that provide service on their behalf comply with related laws and regulations, such as the laws on data privacy, the laws on anti-money laundering, the laws on exchange control and the Bank of Thailand's	objectives, and periodically performs service impact analysis and risk assessment to determine key service processes and recovery objectives. It also has a detailed business continuity plan and disaster recovery strategy, and conducts regular drill tests to ensure their effectiveness. In addition, HUAWEI CLOUD has developed business continuity management regulations and incident response policies based on industry standards and advanced requirements, provided training for key positions, and regularly updated disaster recovery plans. HUAWEI CLOUD sets risk management objectives in compliance with the cost-effectiveness principle, formulates management mechanisms and detailed operation rules for HUAWEI CLOUD risk assessment, risk ceiling, and risk handling, comprehensively assesses risks in the business domain every year, specifies risk contact persons or risk handling owners for identified risks, and formulates risk handling solutions. Different levels of risk specify disposal requirements for different periods of time. HUAWEI CLOUD Legal Affairs Dept is responsible for identifying laws and regulations on cyber security, privacy protection, and intellectual property rights applicable to HUAWEI CLOUD services and updating supervision requirements every year. In addition, HUAWEI CLOUD conducts annual cyber security compliance inspections, including serious issues found in business self-checks, technical assessments, and audits, as well as external requirements, including compliance requirements of external supervision, security and privacy requirements raised by customers, implementation of supervision requirements, and industry crises. Report the inspection and rectification results to the BOD and corporate senior management to ensure that the identified issues are resolved and finally closed.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		notification on market conduct. (4) Financial institutions must ensure that all levels of subcontractors from business partners must also comply with regulations and conditions required in 5.3.1-5.3.2.	
5.5	Audits by Bank of Thailand, external auditors or other regulatory bodies	Financial institutions must ensure that the Bank of Thailand, external auditors, or other official organizations can audit business partners that provide service on behalf of financial institutions, or subcontractors (if any) and also have available accurate and current data related to service used for audit.	FIs must use the Bank of Thailand, external auditors or other official organizations to audit their business outsourcing service providers and also have accurate and up-to-date data related to the services used for the audit. HUAWEI CLOUD's cloud services and platforms have obtained numerous international and industry security compliance certifications, covering information security, privacy protection, business continuity management, and IT service management. HUAWEI CLOUD is committed to building secure and reliable cloud services for customers from all walks of life. Enable customers' business, add value, and escort. To help customers meet compliance requirements, HUAWEI CLOUD regularly reviews and updates all system documents every year based on the requirements of the internal management system. In addition, HUAWEI CLOUD has a dedicated team to maintain the product description and operation manual of cloud services. At least English documents are provided on the international website. In addition, HUAWEI CLOUD is audited by professional third-party audit organizations every year and provides dedicated personnel to actively respond to and cooperate with the audit activities initiated by the customer. In addition, HUAWEI CLOUD provides after-sales service assurance for customers. The professional service engineer team of HUAWEI CLOUD provides 24/7 service support.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Customers can seek help through work orders, intelligent customer service, self-service, and hotline to escalate problems. In addition to basic support, enterprise customers with complex systems can choose the applicable support plan to receive dedicated support from IM Enterprise Groups, Technical Service Managers (TAMs), Service Managers, and more.
Attachment 3	Business Partner Selection Guide	Financial institutions must set out guidelines on appropriate business partner selection prior to entering into contracts or agreements or review to extend contract or agreement. Financial institutions must set out the guidelines on business partner selection according to the level of risk and service used, covering key issues as follow. (1) Technical capability, expertise, operational experiences, and readiness to provide service (2) Financial stability (3) Business reputations, complaint history, or prosecution history (4) Organizational culture and service provision policy that is suitable for financial institutions (5) Capability to adapt to new developments (6) Concentration risk that such business partner provides service to many other financial institutions or other	FIs need to develop guidelines for selecting appropriate business partners before entering into contracts, agreements or reviewing extensions of contracts, agreements. These guidelines should consider the following key issues: business partners' technical capabilities, expertise, operational experience and readiness; the financial stability of business partners; Business Partner's business reputation, complaint history or prosecution history; Whether the business partner is appropriate to the financial institution's organizational culture and service delivery policies; Whether the business partner is capable of adapting to new developments; Whether there is a concentration risk that the Business Partner simultaneously provides services to other financial institutions or other persons; and issues related to the guidelines for considering the use of services provided by business partners in relation to directors and officers (conflicts of interest). HUAWEI CLOUD controls and supervises itself according to the cyber security and privacy requirements required by customers. HUAWEI CLOUD will cooperate with financial customers to evaluate their qualifications for providing cloud service outsourcing. Before providing financial outsourcing cloud services, HUAWEI CLOUD will provide standard contracts and service agreement-level non-disclosure agreements to specify the responsibilities, obligations, and service levels of both parties. After providing outsourced cloud services, HUAWEI CLOUD will cooperate with financial

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		persons simultaneously (7) Has guidelines on considering the use of services from business partners that are related to directors and senior managers (conflict of interest)	institutions to inspect their own security systems and provide corresponding evidence or qualification certificates. The inspection contents include supplier security organizations, security R&D testing, and vulnerability management.
Attachment 4	Issues to be included in a business partner contract or agreement	Financial institutions must enter into contract or agreement with business partner in writing, where such contract or agreement should cover key issues at least the following. (1) Details on types of service, scope of responsibility, risk management, internal control system, and security system on storage of financial institutions' assets. (2) Service level agreement to set out minimum service standards that must be carried out, both under normal and not normal circumstances. (3) Business continuity plan to support when service disrupts and cannot be provided continually. (4) Steps in monitoring, auditing, and assessing operational efficiency. (5) Service charge (if any) must be reasonable, with reference from cost or general market rates. It must not offer disproportionate benefits to any persons or juristic persons, both within and outside	FIs must enter into a contract or agreement with the business partner in writing. Such a contract or agreement should cover at least the type of outsourcing business, risk management required by the outsourcing service provider, internal control system and security system, service level agreement (SLA), and business continuity plan. Audit and evaluate the steps of operation efficiency, service fees, contract duration, or contract termination clauses, and information security to maintain the confidentiality and privacy of customer and financial institution data, including requirements for data access rights and ownership, and security incident handling and remediation mechanisms. HUAWEI CLOUD provides the online *HUAWEICLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specify the service content and service level provided and HUAWEI CLOUD's responsibilities. In addition, HUAWEI CLOUD has developed offline contract templates that can be customized based on customer requirements. For example, the independent auditor audits the operation of cloud service providers, and the conditions and responsibilities of HUAWEI CLOUD if services are subcontracted to other suppliers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		business groups. (6) Contract maturity, terms and conditions to terminate contracts, including rights of financial institutions to amend or extend contracts. This is for flexibility in improving service if necessary and also for preventing obstacles for financial institutions' future operation. (7) Scope of responsibility in case of service problems, e.g., service delay or mistakes, and also problem solving directions and redress for losses occurred. (8) Information security, maintaining confidentiality and privacy of customers and financial institutions' data, including access rights and ownership of the data, e.g., data transmission method, data storage method, as well as well-defined penalty should customers and/or financial institutions' data is disclosed. (9) No prevention or prohibition on provision of the same service to other financial institutions. (10) Compliance with regulations set out by the Bank of Thailand as well as other related laws and regulations. (11) Other conditions as appropriate, e.g.,	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		service location, insurance, and use of overseas service. (12) Conditions in permitting business partners that provide service on behalf of financial institutions to subcontract, partly or as a whole, where such subcontractors must comply with guidelines set out in this notification and in agreement with financial institutions. (13) Authorize the Bank of Thailand, financial institutions, external auditors, or other official organization to audit operation, internal control system and request for related data from business partners that provide service on behalf of financial institutions or subcontractors (if any) that is related to such service provided. Should conducting audit requires permission from regulating agencies of the business partners that provide service on behalf of financial institutions, financial institutions or business partners that provide service on behalf of financial institutions must take action to ensure that audit can be carried out legally.	

10 How HUAWEI CLOUD Meets the Requirements of BoT Regulations on the IT supervision of payment systems and services providers

10.1 Information Technology Risk Management Standards

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5.1.1	Formulation of system security standards	Information Technology (security baseline and hardening) Set a minimum-security baseline and set security hardening to include operating systems database systems "Application: Network devices and network security devices that support the system clearly and in writing, including reviewing and reviewing as required. If there is a failure of service providers and business operators to comply with the standards, a request process must be established." Approve an exception (exception) to assess risks and consider adequate risk control guidelines before taking action.	Payment system service providers need to establish information technology security policies and standards within their organizations, standardize minimum security standards for operating systems, database systems, applications, network devices, and network security devices, and establish security guarantees for the services they provide. As a cloud service provider, HUAWEI CLOUD has obtained many international and industry security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, and CSA STAR. HUAWEI CLOUD complies with international standards to establish an information security management system, an IT service management system, and a business continuity management system, and implements the system requirements in daily operations. In addition, HUAWEI CLOUD regularly conducts risk assessment and management review activities every year to identify problems during system operation, implement rectification, and promote continuous improvement of the management system.
5.1.2	Malware Protection	Providing tools to prevent malware threats and keeping up-to-date	Customers should have safeguards in place to protect against malicious attacks or intrusion events, including intrusion

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		with new threats to mitigate the risk of malware attacks.	prevention and detection, antivirus, and malware protection. In addition, Customer should develop and implement policies and procedures to subscribe to threat intelligence and share and validate information related to cyber attacks, including virus and/or malware attacks, with external parties. On the office network, HUAWEI CLOUD deploys the IPS, WAF-Web Application Firewall (WAF), and antivirus software to prevent malicious software from being attacked. In addition, HUAWEI CLOUD deploys the HIDS host-based intrusion detection system to manage vulnerabilities of system components and networks. The IPS can detect and prevent potential network intrusions. Web application firewalls are deployed at the network border to protect application software from external attacks such as SQL injection, CSS, and CSRF. Antivirus software provides antivirus protection and firewalls in the Windows system. The host-based intrusion detection system (HIDS) protects ECSs and reduces the risk of account theft. It provides functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page anti-tamper. HUAWEI CLOUD continuously provides security awareness education for employees during their on-the-job years. There is a dedicated information security awareness training program, including malware prevention.
5.1.3 Security Patch Management	Risk Management	Institute a security patch management process for all systems and devices to mitigate the risk of information technology systems being attacked by new vulnerabilities. This must be completed in a timely manner according to the vulnerability level and	Customers should take steps to monitor installed updates and patches for systems or applications within the organization so that any outdated, vulnerable updates and patches can be identified in a timely manner. The customer is responsible for the security configuration and management tasks (including updates and security patches) necessary to deploy cloud services such as virtual networks, virtual host and guest virtual

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		security level. If a system or device manufacturer has not formally notified security patches to close newly discovered vulnerabilities, service providers and business operators must provide alternative controls to reduce the risk of being attacked by the vulnerabilities. However, if a security patch cannot be installed, an exemption approval process must be established. Risk assessment, including consideration of adequate risk control guidelines	machines, and containers. HUAWEI CLOUD has established a security vulnerability management process. Vulnerability administrators and related security roles are responsible for vulnerability assessment. In addition, HUAWEI CLOUD has specified vulnerability grading, responsibility assignment, and vulnerability handling requirements for periodic installation of key security patches to reduce vulnerability risks. In addition, HUAWEI CLOUD has set up a dedicated vulnerability response team to evaluate and analyze the causes and threat levels of vulnerabilities in a timely manner, formulate remedial measures, and evaluate the feasibility and effectiveness of remedial measures.
5.1.4	Privileged User Account Management	Strictly regulate the use of privileged user accounts, such as assignment of withdrawal rights, validation periods, post-use review, setting strong passwords of operating systems, database systems, work systems, network devices, and network security devices, to prevent User accounts with high privileges used without permission.	Customers should develop a privileged account management mechanism to control and restrict the allocation and use of privileged access rights. Strict login/use approval requirements and processes shall be set for administrator accounts or super administrator accounts. Administrator accounts can be logged in only after being approved by senior management in the organization. HUAWEI CLOUD follows the principles of SOD and rights checks and balances to separate incompatible responsibilities and implement reasonable rights division. In addition, HUAWEI CLOUD has developed the SOD management matrix to help implement this management principle. HUAWEI CLOUD uses the log system to monitor administrator-level access and prevent non-administrator employees from having more rights than they should have, such as privileged access. HUAWEI CLOUD emphasizes that the security risks of employee cloud service accounts are controllable, and requires strong passwords. The account

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			permission scope is regularly reviewed. Privileged accounts are strictly managed and reclaimed. Employees are identified using multi-factor authentication every time they log in. HUAWEI CLOUD uses the log system to monitor administrator-level access and prevent non-administrator employees from having more rights than they should have, such as privileged access. HUAWEI CLOUD will not touch customer data unless necessary services are provided for customers or binding orders issued by government agencies to comply with laws and regulations.
5.1.5	Multifactor Authentication	Provide multi-factor authentication in the following cases: (1) All privileged user accounts of the operating system, database system, work system, network device and network security device; (2) Every user account that has access to customer information of systems, operations, database systems, work systems, network devices and network security devices connected to the Internet facing network. If operating systems, database systems, work systems, network devices, and network security devices do not support multi-factor authentication, service providers and business operators can use other methods that are equally effective to reduce the risk of a simple authentication attack. However, if this	Customers should establish identity and access control policies and implement appropriate technical and administrative measures to prevent unauthorized access to information assets, which may include remote access mechanisms, logging, etc. HUAWEI CLOUD emphasizes that the security risks of employee cloud service accounts are controllable, and requires strong passwords. The account permission scope is regularly reviewed, and privileged accounts are strictly managed and reclaimed. IAM is used to manage access. Multi-factor authentication is supported for login verification and operation protection. Employees need to use multi-factor authentication to determine their identities every time they log in.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		is not possible on some systems or devices, procedures must be provided. Approval of exemptions and risk assessment and consideration of appropriate risk control guidelines.	
5.2.4	Compliance with laws and regulations related to information technology	To ensure compliance with relevant laws and guidelines on information technology (IT compliance), such as the Electronic Transactions Law, Computer Offenses Law, Cyber Security Law, or the Personal Data Protection Law to prevent violations or non-compliances. Rules of the relevant departments and supervision.	Customers should develop a security compliance review process to regularly review the organization's information security and cyber security compliance to ensure that it complies with and updates the latest security-related laws, regulations, and/or guidelines applicable to the organization. HUAWEI CLOUD's cloud services and platforms have obtained numerous international and industry security compliance certifications, covering information security, privacy protection, business continuity management, and IT service management. HUAWEI CLOUD is committed to building secure and reliable cloud services for customers from all walks of life. Enable customers' business, add value, and escort. To help customers meet compliance requirements, HUAWEI CLOUD regularly reviews and updates all system documents every year according to the requirements of the internal management system. In addition, HUAWEI CLOUD has a dedicated team to maintain the product description and operation manual of cloud services. At least English documents are provided on the international website. As an outsourcing service provider of financial institutions, HUAWEI CLOUD presents its best practices on risk management and customer protection in white papers or compliance documents. Customers can visit the Trust Center on their official website to view related best practices. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with the audit requirements

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			initiated by the customer. The customer's rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with the customer based on the actual situation. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, such as ISO27001, ISO27017, ISO27018, SOC, and CSA STAR. HUAWEI CLOUD is audited by a third party every year.

10.2 Notify or report to BoT

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Charter 7	Notify or report to BoT	In order for the BoT to be able to monitor and monitor the information technology risk and overall financial risk of Service Providers and Operators, Service Providers shall promptly notify Service Providers and Operators of information technology issues or cyber threat events, as follows: 7.2 Reporting Information Technology Issues: The service provider must report to the BoT. Significant issues or incidents that affect their services, work systems or reputation in the course of their use of information technology, as well as attacks or threats to important information technology from cyber	Payment system service providers report to the BOT information technology risk and overall financial risk of their organization, as well as identified information technology issues or cyber threat incidents. The payment system service provider shall establish a security incident management and reporting mechanism, report to the company's management in a timely manner after a security incident occurs, and report to the BOT major issues or events that affect its services, working systems or reputation during the use of information technology, as well as attacks or threats to important information technology from cyber threats. Payment system service providers must report to the BoT on a quarterly basis, in accordance with the format and channels specified by the BOT, on the use of services (outsourced, etc.), connection or access to important third party information. HUAWEI CLOUD has developed a security event management mechanism and continuously optimizes the mechanism. The security incident response process clearly defines the roles and responsibilities that are responsible for each activity during the incident response process. HUAWEI CLOUD Big Data Analytics can quickly collect,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		threats, and problems or incidents reported to management. The Service Provider must report such issues or incidents to the BoT at its highest location. When an accident occurs or a problem or event is found, it should be confirmed through the BoT channel immediately. Determine the cause and provide further solutions later. If the Underwriter or the Underwriter has a problem or significant incident in the use of the information technology referred to in paragraph 1, the Underwriter or the Underwriter shall report the problem. Information technology in accordance with Article 4.2.3(5.2.1) of the Notice on Regulatory Rules for Conducting Businesses in Financial Transaction Systems and Article 4.2.3(8.3) of the Notice on Regulatory Rules. (as appropriate) and oversee its payment services business. 7.4 Important Third Party Reports: Significant currency payment system providers, currency payment system operators under transaction accounts and currency payment	process, and analyze massive logs in real time. It can interconnect with third-party security information and event management (SIEM) systems, such as ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components. The system continuously monitors and analyzes security events in real time to detect security events in a timely manner. In addition, HUAWEI CLOUD has a 7 x 24 professional security incident response team and a corresponding security expert resource pool to handle security incidents. HUAWEI CLOUD defines security event grading and escalation principles, levels security events based on the impact of security events on customers' services, and initiates the customer notification process based on the security event notification mechanism to notify customers of the events. When a serious security incident occurs and has or may have serious impact on a large number of customers, HUAWEI CLOUD can notify customers of the incident information through bulletins as soon as possible. Describe the incident, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer. After the incident is resolved, an incident report will be provided to the customer on a case-by-case basis. HUAWEI CLOUD's cloud services and platforms have obtained many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, and IT service management. HUAWEI CLOUD is committed to building secure and reliable cloud services for customers from all walks of life. Enable customers' business, add value, and escort. To help customers meet compliance requirements, HUAWEI CLOUD regularly reviews and updates all system documents every year according to the requirements of the internal management system. In addition,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		service operators under significant transaction accounts must submit reports. Use the Services, connect to or access important third-party information on a quarterly basis in accordance with the formats and channels specified by BoT.	HUAWEI CLOUD has a dedicated team to maintain the product description and operation manual of the cloud service. At least English documents are provided on the international website. In addition, HUAWEI CLOUD is audited by professional third-party audit organizations every year and provides dedicated personnel to actively respond to and cooperate with the audit activities initiated by the customer.

11 How HUAWEI CLOUD Meets the Requirements of OSEC <Rules in Detail on Establishment of Information Technology System> and <Guidelines for Establishment of Information Technology System>

Rules in Detail on Establishment of Information Technology System 2023 (Rules) are the management requirements for enterprise IT governance and information security provided by the Office of the Securities and Exchange Commission of Thailand (OSEC) for operators engaged in securities services (hereinafter referred to as "operators") in the construction of information technology systems. *Guidelines for Establishment of Information Technology System 2023 (Guidelines)* is a further interpretation of the management requirements of the *Rules*, and provides precautions and best practices to meet the management requirements.

Rules provide operators with IT governance, IT security, and IT system audit requirements for information technology system construction through *Annex 2 Information Technology Governance, Annex 3 Information Technology Security, and Annex 4 Information Technology Audit.*

When operators comply with the preceding regulations, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following section summarizes the control requirements related to cloud service providers in the *Rules* and its attachments and *Guidelines,* and describes how HUAWEI CLOUD, as a cloud service provider, helps intermediaries meet these control requirements.

11.1 The Rules in Detail on Establishment of Information Technology System 2023

Articles 4, 5 and 6 of *The Rules in Detail on Establishment of Information Technology System 2023* require operators to conduct governance, security management and information technology audit of information technology systems in accordance with the contents of Annexes 2, 3 and 4, and to conduct risk level assessment of information technology systems in accordance with the requirements of OSEC every year. Relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4 & 6	Risk Level	4. In the interest of complying with the regulations specified in	FIs are required to assess the risk impact of their internal

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	Assessment RLA	this Notification, a business operator shall conduct an assessment of information technology systems' impact on the business operation of the business operator according to the RLA (Risk Level Assessment) form, and submit the results of such assessment to the SEC Office within the fourth quarter of each year according to the form and procedures specified on the website of the SEC Office. The results of the RLA under Paragraph 1 shall be considered by the Board of Directors or the person assigned by the Board of Directors to be in charge of the matter. 6. In assessing the risk level related to information technology systems (RLA) as specified under Clause 4 for the year 2023, a business operator shall perform the following acts: (1) assessing the risk level and submitting the results of the first assessment to the SEC Office within 31 July 2023; (2) assessing the risk level and submitting the results of the second assessment to the SEC Office within 31 December 2023.	information systems on their business based on the Risk Level Assessment Form (RLA) published on the official website of the Office of the Securities and Exchange Commission (OSEC) and submit an RLA report to OSEC in the fourth quarter of each year. Before submission, the RLA shall be reviewed by the board of directors of the institution or the designated responsible person of the institution. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with the customer based on the actual situation. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, such as ISO27001, ISO27017, ISO27018, SOC, and CSA STAR. HUAWEI CLOUD is audited by a third party every year.

11.2 Annex 2 Information Technology Governance

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Part 1	Roles and responsibilities of the Board of Directors	A business operator shall ensure that IT risk governance will be supervised by its board of directors to ensure that the IT risk is aligned with risk appetite, taking into consideration the enterprise risk management (if any). The business operator shall at least address the following	Customers should specify the information security organization, define information security roles and responsibilities, and establish a mechanism for separation of duties or cross-check of information security. Huawei regards cyber security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		matters: 1.1 Establishment of an IT governance framework and oversight of IT plans, ensuring the IT plans will conform with business plans and be sufficiently appropriate for accommodating future IT changes and business operation changes; 1.2 allocation of appropriate and sufficient IT resources and IT personnel for business operation; 1.3 stipulation of written policies related to IT risk supervision, which shall at least cover the policies prescribed in Clause 2.2 of Part 2; 1.4 establishment of processes and procedures for IT risk management and IT security to be in line with policies in Clause 1.3, including ensuring appropriate implementation thereof; 1.5 creation of knowledge and awareness of IT risk for directors and personnel continuously and effectively; and 1.6 monitoring, reviewing, and reporting on the conformance of the policies in Clause 1.3 to the board of directors at least once a year. In case of the occurrence of any incident or change that may significantly affect the conformance of such policies, the board of directors shall be informed without delay.	as one of the company's important strategies and implements it through a top-down governance structure. In terms of organization, the top management of HUAWEI CLOUD is responsible for deciding and approving the overall cyber security strategy of the company. The HUAWEI CLOUD security management department is responsible for developing and implementing Huawei's end-to-end cyber security assurance system. The HUAWEI CLOUD security management department directly reports to the CEO of Huawei. The HUAWEI CLOUD information security management system has established a SOD mechanism to implement SOD. HUAWEI CLOUD implements role-based access control permission management for internal personnel. Personnel in different positions and responsibilities can only perform specific operations on authorized objects. Ensure that personnel do not use network analysis and monitoring tools without authorization through minimal permission assignment and strict behavior audit.
Part 2	Organizational IT Risk Governance	A business operator shall establish an IT governance framework that shall at least contain the following features: 2.1.1 enabling independent checks and balances; and 2.1.2 being in line with the three Lines of Defense (3LoDs) concept, under which IT-related duties are clearly segregated as follows:	Customers should establish an IT governance framework that adheres to the 3LoD three lines of defense and clearly delineates IT-related personnel responsibilities. At the same time, the customer shall develop a sound information technology risk supervision policy and relevant procedures and processes for implementing the policy in

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		1st Line of Defense: Operations 2nd Line of Defense: Risk management and compliance with applicable laws and regulations; and 3rd Line of Defense: Audit A business operator shall establish policies on IT risk supervision in writing which shall be approved by its board of directors or the committee assigned by the board of directors, as follows: 2.2.1 IT risk management policy: (1) Roles and responsibilities of related persons in IT risk management; (2) Establishment of IT risk management process to ensure the risk will be in line with the organization's risk appetite. 2.2.2 IT security policy: (1) Organization of IT security; (2) Personnel and third-party management; (3) IT asset management; (4) Data security; (5) Access control; (6) Cryptographic control; (7) Physical and environmental security; (8) IT operations security; (9) Communication system security; (10) IT project management, system acquisition, development and maintenance; (11) IT incident management; (12) IT contingency plan. A business operator shall operate according to the policies in Clause 2.2, as follows: 2.3.1 Communication of policies under Clause 2.2 to related persons for acknowledgement in	accordance with the detailed rules, and review and update the policies, processes and procedures at least annually. HUAWEI CLOUD inherits Huawei's risk management capabilities and establishes a risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD effectively controls risks in complex internal and external environments and huge uncertain markets, strives to balance performance growth and risks, and continuously manages internal and external risks. Ensure the sustainable and healthy development of the company. In addition, HUAWEI CLOUD builds an information security management system based on ISO27001 and formulates an overall information security strategy for HUAWEI CLOUD. The strategy specifies the architecture and responsibilities of the information security management organization, management methods of information security system documents, and 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. Protect the confidentiality, integrity, and availability of customer systems and data. In addition,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		accordance with their roles, responsibilities, and data access rights in an easily accessible manner to enable such related persons to understand and comply with the policies properly; 2.3.2 Establishment of operational processes and procedures in compliance with the policies under Clause 2.2; 2.3.3 In the event of changes in the policies under Clause 2.2, such changes shall be communicated to all related persons and the operational processes and procedures shall be revised to be in line with such changes. A business operator shall review or revise the policies under Clause 2.2 at least once a year and without delay upon occurrence of any incident that may significantly affect the governance and management of IT risk.	HUAWEI CLOUD focuses on the security awareness development of employees and outsourcing personnel, and formulates and regularly implements the security awareness training plan.

11.3 Rules - Annex 3 Information Technology Security & Guidelines – Annex IT System Construction Guide

Annex 3 Information Technology Security of the *Rules* and the Annex IT System Construction Guide of the *Guidelines* provide detailed rules and guidelines for securities business operators to build a secure information technology security system from 12 information security management system control domains.

11.3.1 Organization of Information Technology Security

Information Technology Security Part 1 & IT System Construction Guide Clause 2.1, A business operator shall ensure there is such organization which shall at least contain the following features:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology	Organization of Information	1.1 establishing an organizational structure for IT operations with	Customers should clarify the information security internal organization, define information security roles and responsibilities, and establish a

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Security Part 1 & IT System Construction Guide Clause 2.1	Technology Security	details of duties and responsibilities of the personnel in writing; and 1.2 establishing a cross-check for IT operations to prevent potential risks.	mechanism related to segregations of duties or cross-check for information security. Huawei prioritizes cybersecurity as one of the company's key strategies, and implements it top-to-bottom through its entire governance structure. From an organizational structure perspective, top management of HUAWEI CLOUD is responsible for making decisions on and issuing approvals of the company's overall cybersecurity strategy. HUAWEI CLOUD security management department is responsible for formulating and executing Huawei's end-to-end cybersecurity framework. The security management department reports directly to the company's CEO. HUAWEI CLOUD has established a responsibility separation mechanism to separate internal responsibilities and authorities. HUAWEI CLOUD implements role-based access control rights management for internal personnel. This limits personnel permissions to only allow the operations which are required for their individual role. While minimizing permission allocation and implementing strict behavioral auditing, it ensures that employees are not unauthorized to use network analysis and monitoring tools.

11.3.2 Personnel and Third-Party Management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 2 & IT System Construction Guide Clause 2.2	Personnel and Third-Party Management	2.2.1 Personnel subject to management 2.1 Related personnel or those who use IT systems to perform their work. Management A business operator shall conduct personnel management under Clause 2.1 appropriately by at least undertaking the following acts: (1) having a process for personnel selection as follows:	Customers should establish an information security management system related to their cloud service provider and specify information security requirements when using cloud services. HUAWEI CLOUD provides online version of *HUAWEI CLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		(1.1) considering knowledge, competence, and adequacy in the operation; and (1.2) checking background of personnel prior to employment sufficiently and in line with the risk of the position and duties and responsibilities thereof. (2) requiring the personnel to understand, acknowledge and affix their signature for acknowledgement of the following matters: (2.1) the roles and responsibilities of such personnel in relation to IT security; and (2.2) non-disclosure agreement; (3) raising awareness of IT risk among personnel who can access data or application systems within the organization so the personnel could use the application systems safely; (4) requiring personnel to refrain from using the IT systems in such a manner that will cause damage to the capital market or that is illegal, or violates requirements or code of conduct established by the business operator (if any); (5) establishing disciplinary action policy for responding to personnel violating or failing to comply with IT security policies and measures; and (6) establishing a procedure to be undertaken upon the end of employment or change in the position in order to prevent potential breach or damage to IT assets. 2.2.2 Third-Party Management Personnel subject to management 2.2 Third parties are subject to management if the business operator undertakes any of the following acts: 2.2.1 using IT services from third	the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. For example: auditing the cloud service provider's operation through an independent auditor; or, conditions and responsibilities for HUAWEI CLOUD when subcontracting services to other suppliers. At the same time, customers need to take a series of measures to ensure IT security and protect sensitive data when managing people or people working with IT systems and working with third parties. Specific measures include background checks and non-disclosure agreements, raising awareness of IT risks within the organization, developing disciplinary policies, and establishing exit procedures. Evaluate and manage third parties, sign non-disclosure agreements, monitor and manage third parties' service usage, maintain IT security, and prepare for IT incidents. HUAWEI CLOUD provides online version of *HUAWEICLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		parties; 2.2.2 connecting its IT system to third parties; or 2.2.3 allowing third parties to access business operator's sensitive data or client data. Management A business operator shall conduct third-party management under Clause 2.2.1, Clause 2.2.2 or Clause 2.2.3 as follows: (1) assess the risk from the use of services, connection, or access of data by third parties, including subcontractors of third parties (if any); (2) establishing practices and criteria for selection of third parties; (3) prescribing roles, duties, and responsibilities of the business operator and the third party clearly and in writing (4) as for the third party who is an IT service provider with the significance as per the outcome of the risk assessment in Clause 2.2 (1), the service agreement or contract shall specify the right for the business operator, the SEC Office, and external auditors appointed by the business operator or the SEC Office to audit the operation and internal control of such third party. If there is necessary cause preventing the business operator from specifying the right to audit pursuant to the first paragraph above in the agreement or contract, the business operator shall have assessment or monitoring measures that are prudent, adequate and in line with the risk and significance of the use of service, connection or data access; (5) having a non-disclosure agreement for third parties or their subcontractors if such persons can	developed an offline contract template, which can be customized according to the needs of different customers. For example: auditing the cloud service provider's operation through an independent auditor; or, conditions and responsibilities for HUAWEI CLOUD when subcontracting services to other suppliers. HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		access business operator's sensitive data or clients data; (6) supervising, monitoring, and managing risks from the use of services, connection, or access to data from third parties which shall be consistent with the risk level and the level of significance of such third parties; (7) maintaining IT security from the use of services, connection, or access to data from a third party to be in line with the business operator's IT security standards; and (8) being prepared to respond to any potential IT incidents with significant impacts to ensure continuity of services or business operations.	CLOUD, such as migrating to local data center. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object StorageMigration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating to local data center.

11.3.3 IT Asset Management

A business operator shall ensure there will be IT asset management to be used for IT security operations in an appropriate, complete and up-to-date manner, as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 3 & IT System Construction Guide Clause 2.3	Asset Management	3.1 developing an IT assets inventory including hardware, software, and hardware and software license; 3.2 designating a person or unit to be responsible for each item of IT assets; and 3.3 providing regular maintenance of IT assets.	Business operators establish IT asset management to ensure that the IT operations of the enterprise are secure, complete, and up-to-date. The specific requirements are as follows: 1. Prepare the IT asset inventory of hardware and software, including its licenses: Enterprises should manage the inventory of all hardware and software, including their license information, so that they can be effectively managed and maintained. 2. Designation of a person or unit responsible for each information technology asset: The enterprise shall designate a person or unit responsible for each information technology asset for its effective management and maintenance. 3. Provide regular maintenance of IT assets: Enterprises should regularly maintain IT assets to ensure their normal

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			operation and security. HUAWEI CLOUD has formulated asset management procedures, specified information asset classification methods and authorization rules for various types of assets, established information asset confidentiality management requirements, specified information asset confidentiality measures taken by HUAWEI CLOUD for information assets at different levels, and standardized asset use. Ensure that the company's assets are reasonably protected and shared. HUAWEI CLOUD uses the asset management system (Cloud Asset Management) to monitor the inventory and maintenance status of information assets on the HUAWEI CLOUD platform recorded on the asset management platform in real time, classify, monitor, and manage information assets, and form an asset list to designate an owner for each asset.

11.3.4 Data Security

A business operator shall maintain data security to ensure its confidentiality, integrity, and availability. as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 4 & IT System Construction Guide Clause 2.4	Data Security	4.1 designation of a person or unit as a data owner 4.2 data classification and guidelines on data security that are in line with the data classification, covering the following data: 4.2.1 data at endpoint; 4.2.2 data in transit; and 4.2.3 data at rest; 4.3 establishment of guidelines for secure data input, data	When processing data, the operator shall take a series of measures to ensure the security, confidentiality, integrity and availability of the data. Specific measures include: 1. Designate an individual or unit as the data owner and specify the ownership and responsibilities of the data. 2. Develop corresponding data classification and security guidelines according to different classifications of data, including end-point data, data in transmission and resting data. 3. Establish guidelines for secure data input, data processing, and data output to ensure data security throughout the process. 4. Prepare a complete and up-to-date data

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		processing, and data disposal; 4.4 preparation of a complete and up-to-date data inventory	inventory that records information about the source, purpose, storage location of all data, etc., in order to manage and monitor the use of the data. 5. Through these measures, operators can better protect the security and confidentiality of data and avoid problems such as data leakage, damage or loss. HUAWEI CLOUD evaluates data security levels based on data confidentiality, integrity, availability, and compliance, and classifies data from severe to slight impacts caused by data damage and leakage. During the design and R&D phase, HUAWEI CLOUD formulates a data flow diagram to display the life cycle of various data in a service and operations performed by Huawei, and specify the operation purpose. For services involving personal data processing in each domain of HUAWEI CLOUD, the business owner regularly sorts out the personal data list involved in the service, and reviews and updates the list every year. HUAWEI CLOUD has established data security management requirements and processes, specified data owners for HUAWEI CLOUD data and tenant data, determined data security levels, and specified data use, security, and privacy protection requirements. HUAWEI CLOUD implements data protection measures and uses proper encryption technologies, recognized security protocols, secure encryption channels, or data encryption on transmission channels.

11.3.5 Access Control

A business operator shall ensure there is efficient access control to prevent the access and revision to systems or data by ineligible or unauthorized persons as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technol	Access Control	5.1 establishing guidelines on management of user	Customers should establish a user access management mechanism to restrict and supervise the access to the system.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
ogy Security Part 5 & IT System Construction Guide Clause 2.5		accounts and access rights by reviewing the right appropriately and regularly in line with the duties and responsibilities, including having a process for removal of the right when such right is no longer needed. 5.2 establishing an authentication process that is suitable for the risk and prevents repudiation; and 5.3 stipulating measures for controlling, limiting, and monitoring privileged users (privileged user management) as follows: 5.3.1 requiring MFA when logging in and changing passwords for the operating systems and the database systems that are related to the critical IT system; 5.3.2 if a business operator has restrictions on MFA, it may use another equivalent method instead and shall conduct risk assessment and consider adequate risk control measures before applying for exception approval; and 5.3.3 implementing strict control and monitoring of the use of privileged user accounts;	Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM) Identity and Access Management (IAM). Except for support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. In addition, HUAWEI CLOUD's Cloud Trace Service (CTS) Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two-factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			responsibilities in different positions are limited to access the equipment under their role. At the same time, when HUAWEI CLOUD O&M personnel access HUAWEI CLOUD Management Network for centralized management of the system, they need to use only identifiable employee identity accounts. User accounts are equipped with strong password security policies, and passwords are changed regularly to prevent violent decryption. In addition, two-factor authentication is used to authenticate cloud personnel, such as USB key, Smart Card and so on. Employee account is used to log on VPN and access gateway to realize the deep audit of user login.

11.3.6 Cryptographic Control

A business operator shall ensure there is cryptographic control that is reliable and in line with international standards by stipulating a secure method for encryption and key management to ensure that the confidentiality, integrity and authenticity of data are appropriate and efficient, as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 6 & IT System Construction Guide Clause 2.6	Cryptographic Control	6.1 stipulating secure encryption method; 6.2 establishing cryptographic key management by stipulating control measures for generating, installing, storing, backing up, revoking and destroying cryptographic keys; 6.3 stipulating measures on control of the cryptographic keys provided by a third party which shall be examined to ensure that the generated cryptographic keys are not shared with	When customers use encryption to protect data, they should consider using industry-approved encryption algorithms and key management mechanisms. At the same time, customers should establish cryptographic key management policies and procedures to review cryptographic keys. Currently, services including Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		other users; and 6.4 stipulating an incident response process in the case of leakage of the cryptographic key.	on the cloud. DEW adopts the layered key management mechanism. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to meet users' data security compliance requirements. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with customers' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys. See section 6.8.2 Data Encryption Workshop (DEW) of *HUAWEI CLOUD Security White Paper* for more information.

11.3.7 Physical and Environmental Security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 7 & IT System Construction Guide Clause 2.7	Physical and Environmental Security	A business operator shall put in place physical and environmental security for IT assets, as well as the protection system, and maintenance processes for hardware and facilities related to IT in order to prevent damage to IT assets stored at the primary site, backup site, and the third-party colocation data center.	Customers should develop and implement physical and environmental security management mechanisms. HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standard of *TIA-942 Telecommunications Infrastructure Standard for Data Centers*. HUAWEI CLOUD data centers are located on suitable physical sites, as determined from solid site surveys. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers. See section 5.1 Physical and Environmental Security of *HUAWEI CLOUD Security White Paper* for more information. See section 5.1 Physical and Environmental Security of *HUAWEI CLOUD Security White Paper* for more information.

11.3.8 IT Operations Security

A business operator shall put in place IT operations security measures to ensure that operations related to data processing will be correct and secure. Such measures shall address at least management of the matters as described below.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.1	IT Operations Security	System configuration management by establishing processes for controlling system configurations and regularly reviewing the system configurations to ensure that they are correct and secure.	Customer shall manage the configuration of its systems, establish a system configuration control process, and periodically review the system configuration to ensure that it is correct and secure. The internal security engineering team of HUAWEI CLOUD is responsible for compiling and updating the security configuration specifications of systems and components, and hardening the systems and components in the HUAWEI CLOUD production environment. The HUAWEI CLOUD security event management team spot-checks the compliance of security configurations in the production environment. The HUAWEI CLOUD security event management team is responsible for regularly spot-checking the security configuration compliance of each system or component in the HUAWEI CLOUD production environment based on the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			released security configuration specifications and matching automatic check tools. Currently, HUAWEI CLOUD automatically checks the security configuration baseline in policy-based code PolicyAsCode mode. HUAWEI CLOUD builds a configuration monitoring platform to monitor configuration items of server operating systems, database management systems, and network devices in real time. The monitoring platform compares the actual configuration items with the standard configuration baseline. When a difference occurs, the difference analysis result is automatically sent to the inspection administrator by email for follow-up handling. For details about the security of HUAWEI CLOUD development activities, see HUAWEI CLOUD Security Configuration Guide.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.2	IT Operations Security	Sufficiently-secure change management to ensure that changes will correctly and completely reach the specified objectives and that unauthorized change is prevented.	Customers should establish a documented change management policy and consider formal procedures for managing changes to control changes to IT infrastructure, IT systems, and operational procedures that may impact security. To meet customer compliance requirements, HUAWEI CLOUD has formulated a standardized change management process. Any change to the environment will take place only by orderly management process. After all change requests are generated, they are submitted to the HUAWEI CLOUD Change Committee by the change manager team with change classification assigned. After the committee has reviewed and approved the requests, the planned changes can be implemented on the production network. Before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.3	IT Operations Security	As for capacity management, there shall be measures and processes in place for managing capacity, monitoring system efficiency, and forecasting the use of IT resources in order to ensure that the current business operations are supported and the resource are allocated efficiently for future usage.	Customers should consider establishing formal capacity management standards and procedures to assess and monitor the adequacy of their IT infrastructure, including computer systems, database systems, communication network systems, and IT-related facilities, and monitor their cloud resources to ensure that they can meet business growth requirements. Customers pass through HUAWEI CLOUD's Cloud Eye Service (CES) which provides three-dimensional monitoring of Elastic Cloud Server (ECS),Customers pass through HUAWEI CLOUD's Cloud Eye Service (CES) which provides three-dimensional monitoring of Elastic Cloud Server (ECS), bandwidth, and other resources. The monitoring object of CES is the resource usage data of infrastructure, platform, and application services. CES can currently monitor the following indicators of cloud services: Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Virtual Private Cloud Service (VPC), Relational Database Service (RDS), Distributed Caching Service (DCS), Distributed Message Service (DMS), Elastic Load Balancing (ELB), Elastic Scaling Service (AS), Web Application Firewall (WAF), Host Vulnerability Detection Service (HVD), Cloud Desktop Service (Workspace), Machine Learning Service (MLS), Web Tamper Protection Service (WTP), Data Warehouse Service (DWS), Artificial Intelligence Service (AIS), and so on. These metrics allow users to set alert rules and notification policies to keep abreast of the health and performance of instance resources for each service. HUAWEI CLOUD has also developed a complete performance and capacity management process through early identification of resource requirements, and overall management of platform resource capacity and equipment inventory, HUAWEI CLOUD can continuously optimize resource utilization and resource availability levels, and ultimately ensure that cloud resources meet the business needs of users.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.4	IT Operations Security	Server and endpoint security are aimed at protecting such devices from being used as a channel for data leaks or unauthorized access to the IT systems.	When deploying the development, test, and production environments, customers must ensure that the environments are physically and logically isolated and strictly manage access to the environments. Huawei's development and test processes comply with unified system (software) security development management regulations and strictly control access to each environment.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.5	IT Operations Security	Stipulation of teleworking, mobile device, and bring your own device (BYOD) security policy and measures by taking into account the related risks and putting in place appropriate control measures.	Customers should establish management procedures and procedures for remote access, mobile device management, and BYOD access to IT systems, establish careful, adequate and appropriate security measures for IT systems and accessed data, and establish adequate security measures for accessed IT systems and data. Risks related to BYOD access must be considered and corresponding risk control measures must be formulated. **Remote Access Control:** HUAWEI CLOUD employees use unique identities on the internal office network. To access Huawei's internal office network from an external network, you need to use a VPN. In O&M scenarios, HUAWEI CLOUD uses VPNs and bastion hosts deployed in data centers to implement unified O&M management and audit on the O&M management platform. External and internal network O&M personnel centrally manage local and remote operations on devices such as networks and servers, implementing unified access, authentication, authorization, and audit for device resource management. To implement remote management of HUAWEI CLOUD, access the bastion host in the resource pool first, and then access related resources from the bastion host, regardless of whether the access is from the Internet or office network. **Mobile Device Management:** HUAWEI CLOUD allows employees to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			use mobile terminals for office work. For mobile terminals, HUAWEI CLOUD has formulated mobile terminal security management regulations, which specify the general requirements for using mobile devices and the mechanism for deleting mobile devices when they are lost. Mobile terminals for office work must register assets and bind them to user accounts. After a terminal is lost, the remote deletion mechanism can be used to delete the terminal data and unbind the terminal data from the account. Mobile devices can access the HUAWEI CLOUD enterprise office environment through internal HUAWEI CLOUD applications. However, HUAWEI CLOUD does not allow mobile devices such as iOS or Android phones and tablets to access the production environment, especially customer content data. HUAWEI CLOUD centrally manages terminals and remotely disables, deletes, and locks software, data, and policies. **BYOD management:** HUAWEI CLOUD does not allow employees to use their own devices to access the HUAWEI CLOUD enterprise office environment. To use their own devices to access the HUAWEI CLOUD enterprise office environment, you need to apply for and approve the application and install the HUAWEI CLOUD unified terminal device management tool on the devices.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.6	IT Operations Security	Sensitive data should be backed up using an appropriate method and frequency to ensure the availability of data consistent with the goal of restoring the IT system where the IT system and primary data were interrupted or damaged. Backup copies of data and the data recovery process shall be tested at least	Customers should establish a backup management mechanism to back up key business data, operating system and software application. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also back up

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		once a year.	data through HUAWEI CLOUD's data backup archiving service to ensure that data will not be lost in the event of a disaster. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also back up data through HUAWEI CLOUD's data backup archiving service to ensure that data will not be lost in the event of a disaster. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.7	IT Operations Security	IT system logs shall be produced and stored completely and adequately for use as evidence of electronic transactions. They may also be used for monitoring and reviewing accesses to and uses of data and the IT system as required by law.	Customers should establish a log management process to record and store, as well as to monitor and analyze, the logs of key information systems completely and sufficiently. HUAWEI CLOUD's Cloud Trace Service (CTS)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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. HUAWEI CLOUD also has a dedicated internal audit department that performs periodic audits on O&M activities.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.8	IT Operations Security	Security monitoring involves using a process or tool to prevent and detect IT incidents, malware, or cyber threats which may affect the security of critical IT systems.	Customers should implement a process or tool to detect anomalous events that may compromise the security of their critical IT systems in a timely manner, such as a process or tool to review logs to understand the incident or threat and take appropriate preventive or responsive actions. At the same time, Customer should establish processes or tools to receive cyber threat intelligence to monitor and analyze potential cyber threats and appropriately prevent or address them. HUAWEI CLOUD uses the situational awareness analysis system to associate alarm logs of various security devices and analyze them in a unified manner, quickly and comprehensively identify attacks that have occurred and predict threats that have not occurred. Supports various threat analysis models and algorithms and accurately identifies attacks based on threat intelligence and security consulting. In addition, the system evaluates HUAWEI CLOUD security status in real time, analyzes potential risks, and provides warnings based on threat intelligence to prevent attacks. To ensure the secure and stable running of the HUAWEI CLOUD platform and network, HUAWEI CLOUD takes a series of management measures, including vulnerability analysis and handling. Log monitoring and incident response, optimization of default security configurations of cloud products, deployment of security patches, deployment of antivirus software, and periodic backup of system and device configuration files and testing their effectiveness. HUAWEI CLOUD sets detection tools, threat signatures, and attack indicators for all possible threats to HUAWEI CLOUD systems, applications, and networks, and updates the detection tools, threat signatures, and attack indicators every week.
Information	IT Operatio	Technical vulnerability	Customers should establish an effective vulnerability management mechanism and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Technology Security Part 8 & IT System Construction Guide Clause 2.8.9	ns Security	assessment of the IT systems shall be conducted in accordance with the risk level to identify vulnerabilities and rectify them to prevent potential cyber threats in a timely manner. The technical vulnerability assessment of the critical IT systems and all internet-facing IT systems shall be conducted at least once a year and upon every significant change to such systems, such as changes to the IT infrastructure or addition of critical functions.	vulnerability assessment plan and perform vulnerability assessment based on the objectives, scope, and requirements of the plan to identify possible vulnerabilities in the system. 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. The Huawei Product Security Incident Response Team (PSIRT) became an official member of the Forum of Incident Response and Security Teams (FIRST) in 2010, through which Huawei PSIRT and the other 471 members can share incident response best practices and other security information. Huawei PSIRT has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD's self-service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations. 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. See section 8.2 Vulnerability Management of *HUAWEI*

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			CLOUD Security White Paper for more information see section 8.2 Vulnerability Management of *HUAWEICLOUD Security White Paper* for more information.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.10	IT Operations Security	8.10.1 A business operator shall conduct penetration testing as follows: (1) internet-facing application systems and network systems: (1.1) at least once a year; and (1.2) upon every significant change to such systems (2) systems other than those in (1): Assessment of risk from intrusions through the internal network shall be conducted to specify the scope of penetration testing and conduct penetration testing as appropriate. 8.10.2 The aforementioned penetration testing shall be carried out by in-house experts or external experts independent of the system owner. 8.10.3 In the event that any vulnerabilities are identified, a business operator shall take steps to rectify them and prevent potential cyber threats in a timely manner to eliminate any risk from such vulnerabilities.	Customers conduct penetration tests on their application systems and Internet-oriented network systems at least once a year, and when major system changes occur. For other systems, the risk of intrusion through the internal network should be assessed and appropriate penetration testing should be performed. Testing should be conducted by internal or external experts independent of the system owner, and once vulnerabilities are discovered, steps should be taken to remediate and prevent potential cyber threats. The operator shall also retain operating reports for at least two years and submit a report of the results of the penetration tests immediately upon notification from the OSEC. The annual business plan of HUAWEI CLOUD includes a penetration test plan. Penetration test personnel must be approved and authorized and perform penetration tests in accordance with HUAWEI CLOUD security penetration test regulations. The penetration test management policies developed by HUAWEI CLOUD define the roles involved in vulnerability scanning and penetration test and the specific work process of each role. Before each penetration test, you need to report and obtain approval from the Chief Security Officer and Regional Security Officer of HUAWEI CLOUD. HUAWEI CLOUD organizes internal and third-party evaluation organizations to scan all systems, applications, and networks of HUAWEI CLOUD every quarter, and hires external third parties to perform penetration tests on HUAWEI CLOUD applications and networks every six months. HUAWEI CLOUD will evaluate and analyze the vulnerabilities found in the penetration test, develop and implement

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		8.10.4 A business operator shall retain reports of operations under Clause 8.10 for a minimum of two years from the date of creation, in a way that such documents are readily available upon request for inspection by the SEC Office. 8.10.5 A business operator shall submit the report on penetration testing results without delay upon notification by the SEC Office.	the vulnerability fixing solution or workaround, and verify the solution after the vulnerability is fixed. If the vulnerability is found, continue to revise the vulnerability fixing solution. If the vulnerability passes the verification, follow the HUAWEI CLOUD change management process. Develop a vulnerability fixing plan based on the vulnerability SLA requirements, implement vulnerability fixing or workarounds, and report the fixing results to the management.
Information Technology Security Part 8 & IT System Construction Guide Clause 2.8.11	IT Operations Security	There shall be patch management by putting in place a process to control the installation of patches on systems and equipment to reduce the risk of potential attacks.	Customers should implement patch management by establishing standards and specifications for patch management to reduce the risk of potential attacks. HUAWEI CLOUD has established a security vulnerability management process. Vulnerability administrators and related security roles are responsible for vulnerability assessment. In addition, HUAWEI CLOUD has specified vulnerability grading, responsibility assignment, and vulnerability handling requirements for periodic installation of key security patches to reduce vulnerability risks. In addition, HUAWEI CLOUD has set up a dedicated vulnerability response team to evaluate and analyze the cause and threat level of vulnerabilities in a timely manner, formulate remedial measures, and evaluate the feasibility and effectiveness of remedial solutions.

11.3.9 Communication System Security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology	Communication System	A business operator shall have appropriate communication system security to	Customers should establish a network communication security management system to ensure that all information located and processed within their network

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Security Part 9 & IT System Construction Guide Clause 2.9	Security	ensure that the communication system and data transmitted through the communication system will be safe and secure and can prevent potential cyber intrusions or threats as well as being able to provide continuous services.	are protected. HUAWEI CLOUD cooperates with customers to exercise supervision over technology outsourcing. The online version of *HUAWEI CLOUD Customer Agreement* defines security responsibilities of cloud service customers and Huawei, while the *HUAWEI CLOUD Service Level Agreement* stipulates the level of products/service provided, including the commitment to service availability and compensation when failing to meet the agreed service level. HUAWEI CLOUD cooperates with customers to exercise supervision over technology outsourcing. The online version of *HUAWEI CLOUD Customer Agreement* defines security responsibilities of cloud service customers and Huawei, while the *HUAWEI CLOUD Service Level Agreement* stipulates the level of products/service provided, including the commitment to service availability and compensation when failing to meet the agreed service level. 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. Customers can use the **Virtual Private Cloud (VPC)**, **Elastic Load Balance (ELB)** to network isolation and load balancing between different regions. Customers can use the **Virtual Private Cloud (VPC)**, **Elastic Load Balance (ELB)** to network isolation and load balancing between different regions. Among them, the VPC service provided by HUAWEI CLOUD for customers can create a private network environment for

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			tenants, and realize complete isolation of different tenants in a three-tier network. Tenants have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation. The ELB automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent.

11.3.10 IT Project Management and System Acquisition, Development, and Maintenance

A business operator shall have IT project management and IT system acquisition, development and maintenance to ensure security throughout the entire life cycle of its IT systems as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 10 & IT System Construction Guide Clause 2.10.1	IT Project Management	Establishing a project management framework to ensure efficient management of significant IT project, ensuring they are delivered accurately and completely as planned and the specified goals are achieved.	Customers should establish the project management framework and detailed project management rules in written form. Under the guidance of corporate strategies, HUAWEI CLOUD formulates mid- and long-term development plans to support the sustainable development of HUAWEI CLOUD services, and formulates annual business plans and implementation path diagrams. It includes cyber security activities, compliance requirements of applicable laws and regulations, and personnel and resources for carrying out and establishing various cyber security projects to ensure the effective implementation of cyber security strategies. HUAWEI CLOUD reviews network security management policies and plans at least once a year and updates them as required to reflect changes in business objectives or risk environments. Changes to policies and procedures require senior management approval. In addition, HUAWEI CLOUD has a dedicated audit team to regularly evaluate the compliance and effectiveness of policies, procedures, and auxiliary measures and indicators, and report the investigation results and suggestions to the top management.
Information Technology Security Part 10 & IT System Construction Guide Clause	System Acquisition	Criteria for acquisition of IT systems and service providers shall be established to ensure that the acquired systems meet the business requirements and IT security requirements. The criteria shall take into account the flexibility of changing service	Customers should establish criteria for selecting IT systems and service providers to ensure that the purchased systems meet business needs and information security requirements. HUAWEI CLOUD requires and supervises suppliers based on its cyber security and privacy requirements. HUAWEI CLOUD evaluates the supplier qualification before procurement. Only qualified suppliers can enter the procurement scope of HUAWEI CLOUD.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.10.2		providers, changes in technology, and changes that are significantly related to business operations.	Before the supplier is introduced, the contract and service agreement-level non-disclosure agreement must be signed to specify the responsibilities and obligations of both parties and the service level. After suppliers are introduced, HUAWEI CLOUD inspects the supplier's security agreement execution, capability status, and closed-loop management of issues through the supplier's security system. The inspection covers the supplier's security organization, security R&D testing, and vulnerability management.
Information Technology Security Part 10 & IT System Construction Guide Clause 2.10.3	System Development	Control measures in relation to IT system development including designing, developing, system testing, and deploying the system shall be established to ensure that the system is accurate, secure, reliable, ready for use, and adequately flexible to accommodate usage and aligned with the business plan, by undertaking at least the following acts: (1) establishing detailed requirements of the system and technical specifications of the developed system as follows: (1.1) security; (1.2) availability; and (1.3) capacity. (2) segregating roles and responsibilities of persons involved in system development to ensure that the system will be reviewed before deploying into	Customers should establish a security development management mechanism. Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified, the design engineer will formulate mitigation measures according to the reduction library and the safety design library and complete the corresponding safety design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the design of security test cases, to ensure successful implementation, and ultimately ensure the safety of products and services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		production; (3) segregating the environments of the application systems used for development and testing from production; (4) putting in place a process or tool to ensure secure source code development; (5) conducting testing on the IT system that has been developed or changed to ensure that such system will be able to accurately and comprehensively process data and meet the needs of users; (6) having measures to ensure the integrity of data conversion; (7) having measures to maintain the security and privacy of sensitive data used in testing; (8) conducting a performance test of systems related to electronic channels services or electronic transactions upon significant development or change of the systems, to ensure that such systems able to support the number of concurrent users and transactions in line with business requirements; (9) in the case that a third party is assigned to develop or change IT systems, a business operator shall monitor and ensure that their	HUAWEI CLOUD strictly complies with the security coding specifications of various programming languages issued by Huawei. Static code analysis tools are used for routine checks, and the resulting data is entered in the cloud service tool chain to evaluate the quality of coding. Before all cloud services are released, static code analysis alarms must be cleared to effectively reduce the security issues related to coding when online. HUAWEI CLOUD takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services to ensure that the released cloud services meet security requirements. Testing is conducted in a test environment, isolated from the production environment, and avoids the use of production data for testing. If production data is used for testing, it must be desensitized, and data cleaning is required after use.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		operations comply with the agreement; and (10) having a process for application of approval from management or the committee assigned by the business operator before system deployment.	
Information Technology Security Part 10 & IT System Construction Guide Clause 2.10.4	System Change	(1) Conducting impact assessments and prioritization of change; (2) Establishing a process for requesting change approval, which must be granted in writing by the system owner unit to ensure the necessity for the change has been appropriately considered; (3) Conducting tests before configuring or deploying changes to production to reduce potential risks or impacts; (4) Having a process for approving the release of changes to production from management or the committee assigned by the business operator; (5) Implementing a procedure or tool that controls source code version changes and supports fallback; and (6) Updating supporting documents of application systems that have been	Customers should implement changes to IT systems in accordance with Change Management and Systems Development guidelines. At the same time, customers should always update operating procedures, backup systems, and business continuity plans in response to any IT system changes. In addition, such changes should be communicated to the relevant personnel for confirmation so that the work can be performed correctly. To meet customer compliance requirements, HUAWEI CLOUD has formulated a standardized change management process. Any change to the environment will take place only by orderly management process. After all change requests are generated, they are submitted to the HUAWEI CLOUD Change Committee by the change manager team with change classification assigned. After the committee has reviewed and approved the requests, the planned changes can be implemented on the production network. Before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. HUAWEI CLOUD has also developed a standardized emergency change management process. If emergency changes affect users, they will communicate with users in advance by announcement, mail, telephone,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		changed.	conference, or other means according to the prescribed time limit. If the emergency changes do not meet the prescribed notice time limit, the changes will be upgraded to HUAWEI CLOUD senior leadership, and users will be notified promptly after the changes are implemented. Emergency changes are recorded. The old version and data of the program are retained before the changes are executed. The changes are guaranteed to proceed smoothly through two-person operation to minimize the impact on the production environment. After the implementation, a designated person will verify it to ensure that the change achieves its desired purpose.

11.3.11 IT Incident Management

A business operator shall appropriately and timely manage IT incidents as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 11 & IT System Construction Guide Clause 2.11	IT Incident Management	11.1 provide a point of contact for reporting of IT incidents by personnel, clients, and relevant parties; 11.2 establish a plan or procedure for management of IT incidents; 11.3 reporting IT incidents, personal data breaches, and IT system security incidents that causing damage to client's assets to the responsible person and the SEC Office without delay upon discovery of such incidents; 11.4 conducting a root cause analysis of any IT incident to establish guidelines on resolution and	Customers should establish an information security incident management system. HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		prevention of future recurrence of such incident; 11.5 recording data related to IT incident management and storing such data for a minimum of two years from the date of such incident, in a way that such data are readily available upon request for inspection by the SEC Office; and 11.6 testing and reviewing IT incident management procedures or plans at least once a year. The testing shall cover the management of cyber security threats (cyber security drills). The results of these testing and review shall be reported to the business operator's board of directors or the committee assigned by such board of director.	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. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation. HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate. The test scenarios are combined with the current common network security threats, in which high-risk scenarios will be tested during simulations. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After their completion, relevant personnel will redact a report and summarize any problems identified during the simulation. If the results are indicating issues with the information security incident management and process, related documentation will be accordingly updated. HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			of an emergency and updates it promptly when notified of personnel changes.

11.3.12 IT Contingency Plan

A business operator shall establish an IT contingency plan to address IT incidents that impede normal service or continuous business operations. The business operator shall have the capability to restore the system to its normal state within a reasonable time frame, as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Information Technology Security Part 12 & IT System Construction Guide Clause 2.12	IT Contingency Plan	12.1 appointing a task force or a unit responsible for preparation of an IT contingency plan; 12.2 establishing a process for preparation of an IT contingency plan as follows: 12.2.1 conducting a risk assessment to identify risk scenarios that may disrupt the IT processes and systems, thereby causing the business operator to be unable to provide normal services or operate business continuously; 12.2.2 conducting business impact analysis due to the risk scenarios under 12.2.1 to prescribe the appropriate recovery time objective (RTO), recovery point objective (RPO), and maximum tolerable downtime (MTD); and 12.2.3 preparing a written IT contingency plan approved by the business operator’s board of directors or the committee assigned by such board of directors; 12.3 providing a backup IT system and necessary resources to enable system recovery according to the established recovery time objective; 12.4 communicating the IT contingency plan to relevant personnel to ensure they understand and are able to comply with the IT contingency	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 provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. In order to meet customer compliance

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		plan appropriately; 12.5 reviewing and testing the IT contingency plan at least once a year and upon occurrence of any event that should undergo such review and test. The results of these testing and review shall be reported to the business operator's board of directors or the committee assigned by such board of directors; 12.6 stipulating processes to handle incidents of IT resources overusing or exceeding the capacity of the specified indicators, such as limiting services through certain channels or disconnecting from a service provider or third party that affects the IT system; and 12.7 providing the following contact information to enable efficient coordination of reporting IT incidents or requesting assistance from relevant external agencies, and such information shall be regularly updated: 12.7.1 a list of regulators and third parties that provide services or are connected to the IT systems of the business operator; and 12.7.2 contact channels and a list of relevant persons of the regulators or third parties under Clause 12.7.1.	requirements, HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.

11.4 Rules - Annex 4 Information Technology Governance

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2	Audit Planning and Audit	The audit plan and the audit scope shall be reviewed at least once a year and upon any	The audit plan and scope shall be reviewed at least annually and where necessary.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	Scope Defining	necessary cause requiring such review, to ensure that the scope is aligned with IT risk and the Notification No. Sor Thor. 38/2565.	HUAWEI CLOUD has established an audit management process and performs audits based on the process. The audit management process includes management requirements for audit support plans, risk analysis, security control assessment and summary, rectification plans, reports, review of past reports and related evidence. HUAWEI CLOUD periodically reviews standards such as ISO27001, CSA STAR certification, PCI DSS certification, and SOC reports. HUAWEI CLOUD also reviews the security implementation of HUAWEI CLOUD.
3	IT Audit under the Established Plan and Scope	3.1 IT audit and reporting of IT audit results should be conducted as follows: 3.1.1 In the case of a small-scale business operator, an IT audit should be conducted at least once a year. In any case, an IT audit that covers all rules applicable to the small-scale business operator shall be completed at least once in every two years. 3.1.2 In the case of a low-risk business operator, an IT audit shall be conducted at least once a year. In any case, a full-scope audit covering all applicable rules shall be completed at least once in every two years; 3.1.3 In the case of a medium-risk or high-risk business operator, a full-scope IT audit covering all rules shall be conducted at least once a year;	Information technology audits and reporting of information technology audit results should be conducted in the following manner: 3.1.1 For small business operators, an IT audit should be conducted at least once a year. In any case, an IT audit covering all rules applicable to small business operators should be completed at least every two years. 3.1.2 For low-risk business operators, IT audits shall be conducted at least once a year. In any case, a comprehensive audit covering all applicable rules should be completed at least every two years; 3.1.3 For medium-risk or high-risk business operators, conduct a full-scope IT audit covering all rules at least once a year; 3.2 Audit information shall be documented and documented, such as working papers and audit evidence, for a minimum of two years from the date of creation. These documents shall be stored in such a manner as to make them readily available upon request by the Office of the Securities and Exchange Commission. Huawei has set up a dedicated security audit team to review compliance with global security laws and regulations and Huawei's internal security requirements. Huawei's internal audit team reports directly to the Board of Directors and senior management to ensure that issues

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		3.2 Audit information shall be documented and recorded, such as working papers and audit evidence, for a minimum of two years from the date of creation. The documents shall be stored in a way that they will be readily available for inspection upon request by the SEC Office.	identified are resolved and finally closed. In addition, HUAWEI CLOUD has a dedicated audit team to periodically evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators, and report the investigation results and suggestions to the top management. The management reviews the results and follows up the rectification.
4	Provision of a Plan for Corrective Actions Identified in IT Audit and Progress Monitoring	A plan for corrective actions identified in the IT audit under Clause 3 above shall be suitable to the finding's risk level, and the implementation progress of such plan shall be monitored.	FIs should develop sound audit policies. If problems are found during IT audits, corrective action plans should be developed accordingly. The plan needs to be based on the level of risk found in the survey, that is, the higher the risk, the more stringent the corrective actions need to be taken. At the same time, it is necessary to monitor the progress of the implementation of the plan to ensure that the corrective actions are implemented as planned, thereby reducing risk. HUAWEI CLOUD has set up a dedicated security audit team to review the compliance with global security laws and regulations and internal security requirements of Huawei. Huawei's internal audit team reports directly to the Board of Directors and senior management to ensure that issues identified are resolved and finally closed. In addition, HUAWEI CLOUD has a dedicated audit team to regularly evaluate the compliance and effectiveness of policies, procedures, and supporting measures and indicators, and report the investigation results and suggestions to the top management. The management reviews the results and follows up the rectification.
5	Preparation of and Reports on Audit	5.1 Results of the audit under Clause 3 above and the plan for corrective actions shall be presented to	The audit results and corrective action plans shall be submitted immediately to the Operator's Board of Directors or the Operator's Audit Committee.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	Results	the business operator's board of directors or the business operator's audit committee without delay. 5.2 A business operator shall report the audit results and the plan for corrective actions that have been considered by the business operator's board of directors or the business operator's audit committee pursuant to Clause 5.1 above to the SEC Office in the form and procedure as specified on the website of the SEC Office within the following periods, whichever is due first*: 5.2.1 30 days from the date of presenting the audit report and the corrective action plan to the board of directors or the audit committee; 5.2.2 90 days from the end date of the report under Clause 3 above having been completed; or 5.2.3 three months from the end of the calendar year of the year in which the audit under Clause 3 above commences in the case that the report on the audit results could not be completed within the year of commencement of the	The Operator shall report to the Office of the Securities and Exchange Commission, in the form and procedures prescribed on the Securities and Exchange Commission's website, the results of the audits and corrective action plans considered by the Operator's Board of Directors or the Operator's Audit Committee, within the following time periods, whichever expires first: 30 days from the date of submission of the audit report and corrective action plan to the Board of Directors or the Audit Committee; 90 days from the end date of completion of the report specified in Article 3 above; or 3 months after the end of the calendar year of the year in which the audit begins under Article 3 above, if the report of the audit results cannot be completed within the year in which the audit begins. The audit result report and corrective action plan shall be kept for at least two years from the date of generation, and shall be available for reference at any time upon request by the OSEC Office. HUAWEI CLOUD has developed an internal audit management process to standardize the internal audit principles, audit management process, and audit frequency. A dedicated audit team performs an internal audit on HUAWEI CLOUD once a year to check the operation of the internal control system and evaluate the compliance and effectiveness of policies, procedures, measures, and indicators. In addition, HUAWEI CLOUD regularly hires independent external third parties to provide external audit and verification services. These assessors perform regular security assessments and compliance audits or checks.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		audit. (* Note: For reporting of the audit results for 2023, a business operator shall submit such report within three months from the end of the 2023 calendar year.) 5.3 Audit result report and corrective action plan shall be retained for a minimum of two years from the date of creation, in a way that they are readily available for inspection upon request by the SEC Office.	

12 How HUAWEI CLOUD Meets the Requirements of OSEC Cloud Computing Practice Guide

In November 2019, the OSEC released *Cloud Computing Practice Guide*, which provides FIs with practices to consider regarding the governance of cloud computing services and cloud service provider management. Among them, cloud service provider management includes: assessment and selection of service providers, service agreement, use of cloud computing, service monitoring and evaluation, cancellation and termination of service.

When FIs are seeking to comply with the requirements of *Cloud Computing Practice Guide*, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities stipulated under the requirements. The following content summarizes the compliance requirements related to cloud service providers in *Cloud Computing Practice Guide*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

12.1 Assessment and selection of service providers

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.1	Selection of Service Providers	FIs should clearly define processes and guidelines for selecting cloud service providers and monitoring the availability and appropriateness of the service provider to ensure that the service provider can provide services. In addition, the key factors to be concerned include knowledge, experience, financial	Customers should establish service provider selection criteria. **(1) Technical ability:** HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		capabilities, etc.	industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, HUAWEI CLOUD has created a new multi-computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. **(2) Financial strength:** HUAWEI CLOUD is Huawei's service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. According to the *Market Share: IT Services, worldwide 2019* study released by Gartner, HUAWEI CLOUD ranked sixth in the global IaaS market and one of the top three within China market, with a fastest growth rate up to 222.2% in the world. **(3) Business reputation:** As always, HUAWEI CLOUD adheres to the customer-centric principle, making more and more customers choose HUAWEI CLOUD. HUAWEI CLOUD has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. **(4) Corporate culture and service policies suitable for FIs:** HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, laws and regulations, regulatory requirements in product and service planning, and design phases. Huawei implements these in R&D, and design phases to meet customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and Huawei's comprehensive

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			cloud services.
2.2.1	Assess Information Technology Security Standards	Assess information technology security standards, including data confidentiality, information system integrity, and service availability. For example, the evaluation results of internationally recognized safety standards, such as ISO27001, ISO27017, PCI-DSS, etc.	HUAWEI CLOUD has received a number of international and industry security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, CSA STAR, etc. HUAWEI CLOUD follows international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
2.2.1	Independent Audit	Independent auditors provide assessment and inspection reports, as well as reports on technical safety standards, such as system and organizational control (SOC) reports, which should include key issues of the audit scope, audit period, and audit results.	If an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible personnel to actively cooperate with the audit. Customer audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.
2.2.1	Assess Continuous Service Capability	Assess the continuity practices of cloud service providers and the consistency of business impact analysis of systems that will be used on cloud computing systems, including maximum tolerable downtime (MTD), acceptable recovery time objective (RTO), and recovery point objective (RPO).	To provide continuous and stable cloud services to customers, HUAWEI CLOUD has established a set of complete business continuity management systems in accordance with *ISO 22301 - Business Continuity Management International* standards. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business.

12.2 Service Agreement

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.2	Service Agreement	FIs should consider the following important conditions in service agreements with service providers: A. The agreement between the service provider and the service user shall cover at least the following details: 1. Responsibilities of service providers and responsibilities to intermediaries in the event that service providers fail to comply with the agreement; 2. Operating procedures that comply with internationally recognized information security standards; 3. Measures of information technology security, access control and information disclosure measures; 4. An independent auditor audits the operation of the cloud service provider; 5. Conditions for the cloud service provider to subcontract to other service providers, and the terms of liability for damages that may be caused by the operation of other service providers; B. The information security qualification	Customers should establish an information security management system for their cloud service providers. HUAWEI CLOUD provides online version of *HUAWEI CLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, HUAWEI CLOUD provides online version of *HUAWEI CLOUD Customer Agreement* and *HUAWEI CLOUD Service Level Agreement*, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. For example, auditing of the cloud service provider's operation by an independent auditor; or, conditions and responsibilities for HUAWEI CLOUD when subcontracting services to other suppliers. HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		of the subcontracted cloud service provider is comparable to that of the cloud service provider or meets international standards; C. Monitor, evaluate and review the service performance of cloud service providers; D. The process of for data migration to the new cloud provider in case of any replacement of the cloud provider.	to local data center. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating to local data center.

12.3 Use of Cloud Computing

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.3	Organizational Structure (Internal Organization)	FIs should have multiple channels to contact service providers to deal with use issues and information security incidents.	Customers should establish formal incident and issue management procedures. HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so customers can seek help with methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.
2.2.3	Access Control	FIs should: (1) Formulate appropriate authentication methods, such as multi-factor	Customers can manage user accounts using cloud resources through HUAWEI CLOUD Identity and Access Management (IAM)Identity and Access Management (IAM). Except for the support for password authentication, IAM

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		authentication when accessing the administrator page; (2) The distribution of passwords should be controlled through a formal management process; (3) Assign access rights based on responsibilities, and control user access to information and application system functions according to defined access rights; (4) Monitor and review user access rights.	also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. In addition, HUAWEI CLOUD's Cloud Trace Service (CTS)Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location.
2.2.3	Cryptography	When managing encryption provided by service providers, FIs should collect the following information: ▪ The type of encryption algorithm; ▪ Creation, editing, storage, access, revocation and destruction of keys. Service providers should not be granted access, storage, and management keys.	Currently, services including Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms could be chosen by the customers. Currently, services including Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms could be chosen by the customers. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD Data Encryption Workshop (DEW)DataEncryption Workshop (DEW), which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			mechanism. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to meet users' data security compliance requirements, avoiding unauthorized access 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. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys.
2.2.3	Physical and Environmental Security	FIs should review the destruction procedures to reuse the service provider's equipment or information storage resources.	HUAWEI CLOUD has developed a sound media management process for storage media that stores customer content data in the financial industry to ensure the security of the data stored in the media. 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 applicable laws and regulations, as well as agreement with customers, delete the stored customer data in accordance with data destruction standards. Specific practice is: 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.
2.2.3	Operations Security	If FIs and service providers agree that backup activities are the responsibility of the service provider, FIs shall review the service provider's	HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS)Volume Backup Service (VBS), and Cloud Server Backup

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		implementation of the backup procedure in accordance with the agreement. FIs should determine the requirements for recording events related to cloud computing services, and monitor and store event logs. FIs should review and evaluate service provider's vulnerability management guidelines and install service provider's patches.	Service (CSBS)Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also back up data through HUAWEI CLOUD's data backup archiving service to ensure that data is not lost in the event of a disaster. HUAWEI CLOUD's Cloud Trace Service (CTS)CloudTrace 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; 1. 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; 2. In the storage phase, it adopts multiple backups according to Huawei's network security specifications and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. Huawei 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI CLOUD infrastructure and cloud services, and O&M tools (regardless of whether they are found in Huawei or third party technologies) are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation, and its impact to our customers' services. To protect end users and tenants, HUAWEI CLOUD upholds the principle of responsible disclosure. It ensures no undue risks for potential exploitation and attacks will result from the disclosure of any vulnerability, HUAWEI CLOUD continues to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and tenants vulnerability mitigation solutions, standing shoulder to shoulder with our customers to tackle security challenges caused by vulnerabilities.
2.2.3	Communications Security	FIs should assess and determine the need for network segmentation and tenant isolation in cloud environments, and check the behavior of service providers according to service agreements.	HUAWEI CLOUD cooperates with customers to exercise supervision over technology outsourcing. The online *HUAWEICLOUD Customer Agreement* defines security responsibilities of cloud service customers and Huawei, while the *HUAWEI CLOUD Service Level Agreement* stipulates the level of products/service provided, including the commitment to service availability and compensation when failing to meet the agreed service level. 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. The Virtual Private Cloud (VPC)Virtual PrivateCloud (VPC) service provided by HUAWEI CLOUD for customers can create a private network environment for tenants, and realize complete isolation of different tenants in a three-tier network.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Tenants have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation.
2.2.3	System Acquisition, Development and Maintenance	FIs should conduct information security assessments of cloud computing applications and use them as part of due diligence activities to assess and check the capabilities of cloud service providers. In the case of using SaaS, FIs should evaluate and inspect service providers to establish secure development procedures.	Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management.
2.2.3	Information Security Incident Management	FIs should clarify the following in the incident management regulations: ▪ The types of events that will be reported to cloud computing users; ▪ Detailed information and incident response; ▪ Notify users of the time frame and process of the event; ▪ Contact channel and contact details; ▪ The solution to the problem.	HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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. HUAWEI CLOUD formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation.

12.4 Service Monitoring and Evaluation

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.4	Service Monitoring and Evaluation	FIs should clearly define the roles and responsibilities of follow-up, evaluation and review of services to ensure service contract, service quality performance and identify potential	HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		risks of using services. FIs should monitor, evaluate, and review the services of service providers in accordance with the terms of their agreements ("cloud service agreement") with service providers.	services for customers in all walks of life and providing empowerment and escorting services for customers. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. In addition, HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so customers can seek help with methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.

12.5 Cancellation or Termination of Service

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.5	Cancellation or Termination of Service	When canceling and terminating the use of cloud services, FIs should fully formulate strategies and plans to properly opt out of services to prevent or eliminate the risk of possible adverse effects. For example: risk of service interruption, information security and storage risk.	When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating to local data center. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD, such as migrating to local data center. During the destruction of customer data, HUAWEI CLOUD clears the specified data and all the copies. Once customers agree the deletion, HUAWEI CLOUD

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

13 How HUAWEI CLOUD Meets the Requirements of OIC Guidelines for Governance and Management for information Technology Risk for Life/Non-Life Insurance Companies

The OIC issued the B.E. 2563 Standard on the Governance and Management of Information Technology Risk (IT Risk) in September 2020, which provides (non-life/life) insurance companies in Thailand with practices to consider in the governance and management of organizational information technology risk. Cloud service provider management includes evaluating and selecting service providers, service agreements, and information security incident reports.

When financial institutions comply with the B.E. 2563 Information Technology Risk (IT Risk) Governance and Management Standards, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following section summarizes the control requirements related to cloud service providers in B.E. 2563 and describes how HUAWEI CLOUD, as a cloud service provider, helps financial institutions meet these control requirements.

13.1 Information Technology Security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Clause 23	Third-party service provider or business partner management	In the case that a Company engages third-party management service providers or has business partners, whose systems are connected to its Information Technology system, or	(Life/Non-Life) Insurer customers who have a systematic connection to a third-party managed service provider or business partner or have access to important information, the company needs to develop procedures and criteria for evaluating and selecting third-party managed service providers and employ them under service agreements. Companies require third parties to comply

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		accessible to its important information or that of its customers, the Company must arrange to define procedures and criteria for the assessment and selection of such third-party management service providers, as well as their engagement under service agreements, requirements for their compliance with the Company's security policy, terms of their service level agreements (SLA), and periodic inspection and monitoring of their services. Regarding Information Technology outsourcing, the Company may consider adopting courses of operations in conformity with the Office of the Insurance Commission's practical guideline on criteria for governing Information Technology outsourcing.	with the terms of security policies, service level agreements (SLAs), and regularly check and monitor their services. For IT outsourcing, companies may consider operating in a manner that complies with the Office of Insurance Commission's Practical Guidelines on Managing IT Outsourcing Standards. HUAWEI CLOUD provides online version of ***HUAWEICLOUD Customer Agreement*** and ***HUAWEI CLOUD Service Level Agreement***, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. To cooperate with the customer in supervising the cloud service provider, the HUAWEI CLOUD User Agreement on HUAWEI CLOUD divides the security responsibilities of the customer and Huawei. The HUAWEI CLOUD Service Level Agreement specifies the service levels of HUAWEI CLOUD products/services, including the commitment to service availability. and compensation for services that do not meet commitments.

13.2 Cyber Threat or Information Technology Threat Reporting

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Clause 43	Cyber Threat or Informati	A Company must report Cyber Threats or Information	(Life/Non-Life) Insurance Company customers are required to report cyber threats or information technology threats

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	on Technology Threat Report	Technology threats in the following manner: (1) Reporting to the Office of Insurance Commission promptly upon any occurrence of or acknowledgement of material issues or incidents pertaining to application of Information Technology which impact provision of services, systems, information of insureds, or reputation of the Company, including any attack on the Company's important Information Technology, or any Cyber Threats attacks, as well as issues or incidents that the Company must report to its highest level Executive, with the detailed description and causes of such incidents as well as anticipated impact, action taken to solve issues, the results thereof, the period of issue-solving, and course to prevent future incidents; (2) In the case of any Cyber Threat attack leading to problems or incidents involving the Company's provision of its major information infrastructure service which is a Cyber Threat of low severity, high severity, or critical severity, the Company must inform	in the following ways: First, the Company must promptly report to the Office of the Insurance Commission any significant problem or incident related to the application of information technology, including an attack on the Company's important information technology or any cyber threat attack. Report the detailed description of the problem or event, cause, expected impact, resolution actions, results, problem resolution cycle, and process for preventing future events to the top-level supervisor. Second, if any cyber threat attack results in an issue or incident that is a low-severity, high-severity, or serious-severity cyber threat related to a primary information infrastructure service provided by the Company, the Company must immediately notify the Office of the Insurance Commission or an agency required by law within 72 hours. and provide information to or coordinate with government agencies or any organization established under the Cybersecurity Act to respond to and deal with cyber threats. HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the Office of Insurance Commission or an agency as required by law of such breach without delay, within seventy-two hours, and also provide such information to or coordinate with the government agency or any organization established under the law on Cybersecurity for the Cyber Threats response and handling.	response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation.

14 Conclusion

This whitepaper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in Thailand and shows that HUAWEI CLOUD complies with key regulatory requirements issued by the Bank of Thailand (BoT) and the Office of the Securities and Exchange Commission (OSEC), and the Office of Insurance Commission (OIC). This aims to help customers learn more about HUAWEI CLOUD's compliance status with Thailand 's regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this whitepaper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of the BoT, OSEC

and the OIC on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This whitepaper is for reference only and does not have legal effect or constitute any legal advice. Customers should assess their own use of cloud services as appropriate and ensure compliance with relevant regulatory requirements from the BoT and the OSEC when using HUAWEI CLOUD.

15 Version History

Date	Version	Description
Dec 2024	2.0	Regulatory requirements update
August 2024	1.2	Routine update
April 2022	1.1	Routine update
July 2020	1.0	First release

