HUAWEI CLOUD User Guide to Securities and Futures Industry Regulations & Guidelines in the Hong Kong Special Administrative Region of the People's Republic of China

Issue 01

Date 2020-09-30

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

1.1 Background and Purpose of Publication

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 achieve business model innovate. The Securities and Futures Commission (SFC) of Hong Kong Special Administrative Region of People's Republic of China("Hong Kong SAR, China") is an independent statutory body responsible for regulating the securities and futures markets in Hong Kong SAR, China .To regulate the application of Information Technology (IT) in the securities and futures industry, the SFC published a series of regulatory requirements and guidelines, covering technology risk management and cyber security, use of external electronic data storage and internet trading security management for institutions or organizations (LC) that are permitted to engage in securities and futures-related regulated activities.

HUAWEI CLOUD, as a cloud service provider(CSP), is committed not only to assisting customers of securities and futures industry meeting local regulatory requirements, but also to continuously provide them with cloud services and business operating environments meeting securities and futures industry' standards. This whitepaper sets out details regarding how HUAWEI CLOUD assists customers of securities and futures industry operating in Hong Kong SAR, China in meeting regulatory requirements as to the contracting of cloud services.

1.2 Introduction of Applicable Securities and Futures Regulatory Requirements in Hong Kong SAR, China

- **Use of external electronic data storage:**This policy document sets out requirements where LCs' Regulatory Records are kept with external electronic data storage providers (EDSPs), explains the approval requirements for record keeping and the regulatory standards to be observed by LCs when information is kept or processed electronically using EDSPs.
- **Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading:** This policy document sets out the baseline requirements to

reduce and mitigate hacking risks associated with internet trading. The controls and measures specified in these Guidelines can only reduce or mitigate hacking risks associated with internet trading, but cannot eliminate them. It must be emphasized that these are the minimum standards expected of LCs and are not meant to be exhaustive.

- **Good industry practices for IT risk management and cybersecurity:**This policy document sets out a list of industry practices on technology risk management and cyber security, and LCs that are engaged in internet trading may wish to consider incorporating the good practices listed in it into their IT and cybersecurity risk management frameworks. This list builds on the controls suggested in past circulars and supplements them with recommendations from an external cybersecurity expert based on the latest technological developments.

1.3 Definitions

- **HUAWEI CLOUD**

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

- **External electronic data storage providers(EDSP)**

  EDSPs include external providers of:

  - Public and private cloud services;
  - Servers or devices for data storage at conventional data centers;
  - Other forms of virtual storage of electronic information;
  - Technology services whereby (i) information is generated in the course of using the services and the information is stored at such technology service providers or other data storage providers, and (ii) the information generated and stored can be retrieved by such technology service providers.

- **Internet trading**

  An arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility.

- **Content data**

  Content data refers to data stored or processed during the use of HUAWEI CLOUD services, including but not limited to documents, software, images, audio and video files.

2 HUAWEI CLOUD Security and Privacy Compliance

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

HUAWEI CLOUD has attained the following certifications:

Global standard certification

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

Certification	Description
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict FI certification in the world.
CSA STAR Gold Certification	CSA STAR certification is an international authoritative certification for cloud security level jointly launched by BSI (British Standards Institute) and CSA (Cloud Security Alliance). This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.

Certification	Description
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS 10012 is the personal information data management system standard issued by BSI. The BS 10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
M&O certification	Uptime Institute is a globally recognized data center standardization organization and an authoritative professional certification organization. HUAWEI CLOUD data centers have obtained the M&O certification issued by Uptime Institute. The M&O certification symbolizes that HUAWEI CLOUD data center O&M management has taken the lead in the world.
NIST CSF (Cybersecurity Framework)	NIST CSF consists of three parts: standards, guidelines, and best practices for managing cyber security risks. The core content of the framework can be summarized as the IPDRR capability model including five capabilities: Identify, Protect, Detect, Response, and Recovery.
PCI 3DS	The PCI 3DS standard is designed to protect the 3DS environment that performs specific 3DS functions or stores 3DS data, and supports 3DS implementation. PCI 3DS evaluates the 3D protocol execution environment, including the access control server, directory server, or 3DS server function. and system components, such as firewalls, virtual servers, network devices, and applications, that are required in and connected to the 3D execution environment; In addition, the process, workflow, and personnel management of the 3D protocol execution environment are evaluated.

Regional standard certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Singapore MTCS Level 3 Certification	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires CSPs to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
Gold O&M (TRUCS)	The Gold O&M certification is designed to assess the O&M capability of CSPs who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.

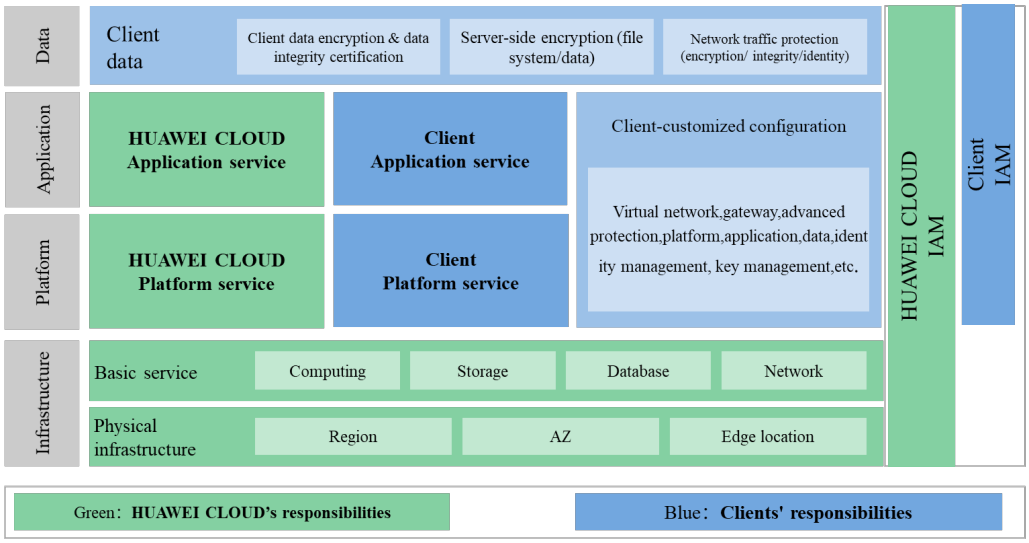
Certification	Description
Cloud Service Security Certification - Cyberspace Administration of China (CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.

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

3 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model



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

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

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

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

For details on the security responsibilities of both HUAWEI CLOUD and customers, 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. For more information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD "**Worldwide Infrastructure**".

5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of SFC Use of external electronic data storage

SFC released *Use of external electronic data storage* on October 31, 2019. This policy sets requirements for the use of external electronic data storage of LC including requirements for keeping regulatory records exclusively with an EDSP, approval of premises for keeping regulatory records, general obligations of LCs using external data storage or processing services.

When LCs are seeking to comply with the requirements provided in *Use of external electronic data storage*, HUAWEI CLOUD, as a CSP, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to CSPs in *Use of external electronic data storage*, and explains how HUAWEI CLOUD, as a CSP, can help customers of securities and futures industry to meet these requirements.

5.1 Requirements for keeping Regulatory Records exclusively with an EDSP

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7(a) (b)	EDSP	A licensed corporation should ensure compliance with the following requirements if it wishes to keep any Regulatory Records exclusively with an EDSP: (a)The EDSP (i) is either a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (Cap 622), in each case staffed by personnel operating in Hong Kong, and (ii) provides data storage to the licensed corporation at a data center located in Hong Kong (Hong Kong EDSP). In addition, the licensed corporation's Regulatory Records which are kept exclusively with the EDSP will be kept at such data center at all times throughout the period in which the Regulatory Records are required to be	If the regulatory record is to be stored with the EDSP, the customer should confirm that the EDSP meets the condition 7 (a) as shown on the left. If the EDSP is not a Hong Kong EDSP as defined in paragraph 7(a), the customer must obtain an undertaking by the EDSP to provide Regulatory Records and assistance as may be requested by the SFC. As a CSP, HUAWEI CLOUD acts as an EDSP in Hong Kong SAR, China and provides data storage services for customers. HUAWEI CLOUD provides services by regions where customers' data is stored. Without authorization, HUAWEI CLOUD never moves customers' data across regions. When using cloud services, customers can select regions for data storage based on the proximity access principle and laws and regulations of different regions. HUAWEI CLOUD has set up a data center in Hong Kong SAR, China for customers to store and process their data locally. To facilitate customer's compliance with this policy and get the approval of such application from SFC under section 130 of the Securities and Futures Ordinance (SFO), HUAWEI CLOUD could provide a signed Undertaking form by using the template in Appendix 1 of the circular upon our customer's request. Meanwhile, a copy of Notice form by using the template in Appendix 2 of EDSP Circular from customer to HUAWEI CLOUD is required before releasing the signed Undertaking form. The Notice is to authorize and request

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		kept by law or regulation. (b)As an alternative, if the EDSP is not a Hong Kong EDSP as defined in paragraph 7(a), the licensed corporation must obtain an undertaking by the EDSP, substantially in the form of the template in Appendix 1 (Undertaking) of this circular, to provide Regulatory Records and assistance as may be requested by the SFC.	HUAWEI CLOUD, as an EDSP, to provide the LC's records to the SFC.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7(c)	EDSP	(c)A licensed corporation should only keep Regulatory Records with an EDSP which is suitable and reliable, having regard to the EDSP's operational capabilities, technical expertise and financial soundness.	Customers should consider their operational capabilities, technical expertise and financial soundness when choosing EDSP. As an EDSP, HUAWEI CLOUD's operational capabilities, technical ability, and financial strength are as follows: **(1)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 implement system requirements in daily operations. 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)Technical ability**: HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, HUAWEI CLOUD has created a new multicomputing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			optimal computing power to maximize customer value. **(3)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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7(d)(f)	Access to the Regulatory Records	(d) The licensed corporation should ensure that all of its Regulatory Records which are kept exclusively with an EDSP are fully accessible upon demand by the SFC without undue delay, and can be reproduced in a legible form from premises of the licensed corporation in Hong Kong approved for this purpose by the SFC under section 130 of the SFO. (f) The licensed corporation should ensure that, irrespective of which EDSP is being used, and of where the EDSP maintains its hardware for the storage of information, Regulatory Records are kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records when it discharges its functions or exercises its powers, taking into account all pertinent political and legal issues in any relevant jurisdiction.	If a customer stores regulatory records exclusively with the EDSP, appropriate measures should be taken to safeguard the regulatory authority's access to regulatory records. To help customers meet regulatory requirements, (1) HUAWEI CLOUD does not use customer data for monetization and explicitly states in the user agreement that it will not access or use the user's content, unless the necessary services are provided to users or to comply with applicable laws and regulations or binding orders of the government institutions. HUAWEI CLOUD strictly conforms to the data protection principles described in Personal Data (Privacy) Ordinance (PDPO). (2) Customers have full ownership over the content they stored in the cloud environment. It's the customer's responsibilities to ensure their content kept in a legible form as well as the data integrity. Customers can store regulatory records in HUAWEI CLOUD's **Object Storage Service (OBS)**to meet relevant requirements. OBS provides users with object-based mass storage that is secure, reliable, and economical. Users can perform a variety of operations (creating, modifying, deleting, uploading, and downloading) to control their objects and buckets. OBS can be used by any type of users – regular users, websites, enterprises, and developers – to store any type of files. OBS supports time-limited access to an object and cross-origin resource sharing (CORS). Time-limited access to an object provides URLs that are accessible within a specified period of time, allowing anonymous users to download software or access other applications. CORS allows configure

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			sharing policies and supports third-party requests for accessing OBS resources. These two function allow customers to provide regulatory records to regulators for access as required.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7(e)	Record and Store Audit Trails	(e) The licensed corporation should ensure that (i) it can provide detailed audit trail information in a legible form regarding any access to the Regulatory Records (including read, write and modify) stored by the licensed corporation at the EDSP, and (ii) the audit trail is a complete record of any access by the licensed corporation to Regulatory Records stored by the EDSP. The audit trail information should be kept for the period for which the licensed corporation is required to keep the Regulatory Records. The access of the licensed corporation to the audit trail information should be restricted to read-only. The licensed corporation should ensure that each user who has accessed Regulatory Records can be uniquely identified from the audit trail.	The customer shall record the access to the regulatory records in a complete manner so as to provide detailed audit trail information displayed in a legible form. The customer should also ensure that the storage time of audit trail information shall not be shorter than that of the regulatory record and that the audit trail information can only be accessed only with readable privileges. To cooperate with customers to meet regulatory requirements, **(1)** The customer may consider storing regulatory records in the **Object Storage Service (OBS)** of HUAWEI CLOUD. OBS can log bucket access requests for use in analysis or auditing. These access logs allow the owner of a bucket to comprehensively analyze the nature and type of requests to access the bucket and identify trends. Once logging is enabled for a bucket, OBS automatically records all access requests into a log file that is written to a user-specified bucket. **(2)Cloud Trace Service (CTS)** of Huawei Cloud can provide cloud service resources operation records to the customer including OBS for query, audit and tracing. The customer can query OBS's access logs in CTS so that the customers can monitor OBS operations including reading, writing, and deleting activities and measure OBS access statistics, trace exceptions and locate problems. The access to the bucket by the authorized user accounts can be identified from the log with time stamps. CTS can merge operation records and generate event files on a regular basis and transfer these to OBS storage bucket, helping the users save operation records with high availability and low cost.

5.2 General obligations of LCs using external data storage or processing services

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
12	Due Diligence	The licensed corporation should conduct proper initial due diligence on the EDSP and its controls relating to its infrastructure, personnel and processes for delivering its data storage services, as well as regular monitoring of the EDSP's service delivery, in each case commensurate with the criticality, materiality, scale and scope of the EDSP's service. Such due diligence should cover: (a) the EDSP's internal governance for the safeguard of the licensed corporation's Regulatory Records (where Regulatory Records are kept with the EDSP), and may include assessing the physical security of the storage facilities, the type of hosting (ie, whether it is dedicated or shared hardware), security over the network infrastructure, IT	Customers should conduct due diligence on EDSP and monitor EDSP service delivery regularly. Due diligence should cover physical security, network security, disaster recovery and business continuity and subcontract management, etc. As an EDSP, HUAWEI CLOUD's situation in the above aspects is as follows: **(1)Physical security**: 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 set 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, reasonable 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		systems and applications, identity and access management, cyber risk management, information security, data loss and breach notifications, forensics capabilities, disaster recovery and business continuity processes; and (b) any subcontracting arrangement by the EDSP for the storage of the licensed corporation's Regulatory Records, especially with regard to cyber risk management and information security.	HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to improve the physical security and environmental safety of HUAWEI CLOUD data centers. **(2)Data isolation:** HUAWEI CLOUD houses data of numerous customers. At the planning stage of each product or component, reasonable isolation mechanism is integrated to prevent unauthorized access and tampering, and to reduce data leakage risks. For example, data isolation is an important feature of HUAWEI CLOUD's storage services such as Elastic Volume Service (EVS), Object Storage Service (OBS), and Scalable File Service (SFS). The implementation of service design varies from service to service. For example, block storage, data storage is isolated by volume (EVS disk). Each volume is associated with a customer ID. The virtual machine (VM) to which the volume is attached must have the same customer ID, helping customers realize data isolation. **(3)Network security capabilities**:Every HUAWEI CLOUD data center has numerous nodes and complex functional zones. To simplify its network security design, prevent the propagation of network attacks in HUAWEI CLOUD and minimize the potential impact of attacks, HUAWEI CLOUD defines both security zones and service planes and implements a network segregation strategy in HUAWEI CLOUD by referencing and adopting the security zoning principle of ITU E.408 and industry

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			best practices on network security. Nodes in the same security zone are at the same security level. HUAWEI CLOUD always takes a wide variety of network security aspects into full consideration ranging from network architecture design to device selection and configuration, as well as O&M. As a result, HUAWEI CLOUD has adopted a set of network security mechanisms to enforce stringent controls and improve cloud security. **(4)Risk Management:** HUAWEI CLOUD complies with Huawei's information security risk management framework, and strictly defines the scope of risk management, risk management organization, and standards in the process of risk management. HUAWEI CLOUD conducts annual risk assessment, and when significant changes emerges in information systems, the company's business, and in applicable laws, regulations or standards, HUAWEI CLOUD will conduct corresponding risk assessments. **(5)Information Security:** According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort. **(6)Disaster recovery and business continuity:** To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems that meets its own business characteristics. 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. **(7)Subcontracting management:** In line with customer supervision for EDSP, the online ***HUAWEI CLOUD Customer Agreement*** divides the security responsibilities of cloud service customers and Huawei, while the ***HUAWEI CLOUD Service Level Agreement*** defines the level of services provided by HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which stipulates that if HUAWEI CLOUD should hire subcontractors, HUAWEI CLOUD shall notify customers and be responsible for the subcontracting services according to customer requirements. HUAWEI CLOUD has developed its own supplier management mechanism and propose security requirements regarding their own products and internal management. In addition, HUAWEI CLOUD will also conduct regular audits of suppliers. Moreover, network security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			agreements are signed with suppliers involved in network security. During the service process, the quality of service will be continuously monitored and the performance of suppliers will be scored. Suppliers with consistently poor security performance will be downgraded. **(8)Identity and access management:** See "Access to the Regulatory Records " and " Record and store audit trails" in 5.1, and "Access Control" in 5.2 of this document. **(9)Data loss and breach notifications:**See "Cybersecurity incident reporting" in 6.3 of this document. See ***HUAWEI CLOUD Security White Paper*** *and* other sections of this document for more information.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
14	Data Encryption	The licensed corporation should also take appropriate steps to ensure that the EDSP protects Relevant Information which is confidential from being intentionally or inadvertently disclosed to, or misused by, unauthorized third parties. To protect its confidential Relevant Information, the licensed corporation should encrypt it while at rest and in transit, or establish effective procedures and mechanisms to safeguard its confidentiality and security. When it is encrypted, the licensed corporation must implement proper key management controls, maintain possession of the encryption and decryption keys	Customers should develop effective procedures and mechanisms to improve the confidentiality and security of data stored in EDSP. If the data is encrypted, the customer should implement an appropriate key management mechanism. As an EDSP, services including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service of HUAWEI CLOUD provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. HUAWEI Cloud provides customers with key management functions for **Data Encryption Workshop (DEW)**that centrally manage keys throughout their lifecycle. Without authorization, others cannot obtain keys to decrypt data, which assists data security on the cloud. DEW adopts the layered key management mechanism. Hardware security module (HSM) adopted by HUAWEI CLOUD creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to support 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Encryption Workshop (DEW) of **Data Encryption Workshop (DEW)** for more information

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
15	Access Control	The licensed corporation should implement appropriate policies, procedures and controls to manage user access rights to ensure that Relevant Information can only be altered for proper purposes by authorised personnel, and is otherwise free from damage or tampering. The sharing of system authentication codes (such as passwords) among users should generally be prohibited, with a view to ensuring that each user who has accessed Regulatory Records can be uniquely identified.	Customers should develop a mechanism for authentication and access management, assign each employee a unique and identifiable account, and realize that employees' access to data is reasonably authorized. As an EDSP: **(1)**HUAWEI CLOUD's unified **Identity and Access Management (IAM)** provides cloud resource access control for customers. With IAM, the customer administrator can manage user accounts and control the access to these user accounts. When multi-user cooperative operation resources exist in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and can also assist the security of user accounts by setting a login authentication strategy, password strategy and access control list. Through the above measures, we can effectively control privileges and provide emergency accounts. Customers can also use the **Cloud Trace Service (CTS)** as a supplement to provide operational records of cloud service resources for users to query, and for audit. **(2)**When HUAWEI CLOUD operators access the HUAWEI CLOUD management network for centralized management of the system, they need to use the only identifiable employee identity account. User accounts are equipped with strong password security policies, and passwords are changed regularly to prevent brute-force cracking. Two-factor authentication (2FA) is also used to authenticate cloud personnel, such as with a USB key, smart card and so on. Employee accounts are

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			also used to log on to the VPN and access gateway to further contain user logins for auditing.
16	Data Confidentiality	Where a licensed corporation is keeping only part of its Relevant Information with the EDSP (whether due to data sensitivity concerns or otherwise), it should put in place controls to prevent the migration of Relevant Information to the EDSP without proper authorization.	Customer should develop monitoring measures to prevent the data from being migrated to EDSP without reasonable authorization. As an EDSP: **(1)**HUAWEI CLOUD does not use customer data for monetization, and explicitly states in the user agreement that it will not access or use the user's content, unless the necessary services are provided to users or to comply with applicable laws and regulations or binding orders of the government institutions. HUAWEI CLOUD strictly conforms to the data protection principles described in Personal Data (Privacy) Ordinance (PDPO). **(2)**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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
17	Allocation of Security Responsibilities	Regardless of how the technology is deployed, the licensed corporation should ensure that the allocation of responsibilities, such as the configuration of security settings, workload protection and credential management, between the licensed corporation and the EDSP is well-defined, clearly understood and properly managed by the licensed corporation.	HUAWEI CLOUD clearly defines the shared security responsibility model with customers, please refer to "3. HUAWEI CLOUD security responsibility sharing model" in this document, or on HUAWEI CLOUD's official website to check the ***HUAWEI CLOUD Security White Paper*** on the specific content of the shared responsibility model.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
19	Business Continuity	A licensed corporation using external data storage or processing services in the conduct of its regulated activities should assess the level of its dependence on the prompt and consistent delivery of services by its service providers as well as the potential operational impact on the licensed corporation and its clients if the services are disrupted. The licensed corporation should establish appropriate contingency plans to ensure its operational resilience, and to require the EDSP to disclose data losses, security breaches, or operational failures which may have a material impact on the licensed corporation's regulated activities.	Customers should assess their reliance on the continuous service provided by EDSP and the possible impact of service interruption. In addition, customers should also develop appropriate contingency plans and require EDSP to disclose security incidents that may have a material impact on the customer's regulated activities. As an EDSP: **(1)**To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems that meets its own business characteristics. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. **(2)**To meet the requirements for post-event notification, HUAWEI CLOUD has developed a complete process for event management and notification. If an event occurs on the HUAWEI CLOUD Base Platform, relevant personnel will analyze the impact of the event according to the process. If the event has or will have an impact on the cloud service customers, HUAWEI CLOUD will start to notify customers of the event. The contents of the notice include but are not limited to description of the event, the cause, impact, measures taken by HUAWEI CLOUD, and measures recommended for customers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
21	Contractual Termination	The licensed corporation should have a legally binding service agreement with the EDSP, which should provide for contractual termination. This may include contractual provisions requiring the EDSP to assist in a transition to a new EDSP or allow a migration of data back to storage at the premises of the licensed corporation and, where relevant, clearly delineate the ownership of the data and intellectual property following termination of the contract.	The customer should sign a legally binding agreement with EDSP, which should provide for contractual termination, such as the transitional arrangements for service termination, and the ownership of data and knowledge products. As an EDSP, **(1)**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. **(2)**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.

6 How HUAWEI CLOUD Meets and Assists Customers to Meets the Requirements of SFC Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

SFC released *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading* onOctober 27, 2017. This policy set the security management requirements of LCs' internet trading from protection of clients' internet trading accounts, infrastructure security management and cybersecurity management and supervision.

When LCs are seeking to comply with the requirements provided in *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*, HUAWEI CLOUD, as a CSP, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to CSPs in *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*, and explains how HUAWEI CLOUD, as a CSP, can help LCs to meet these requirements.

6.1 Protection of clients' internet trading accounts

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
1.4	Data Encryption	A licensed or registered person should use a strong encryption algorithm to: (a) encrypt sensitive information such as client login credentials (ie, user ID and password) and trade data during transmission between internal networks and client devices; and (b) protect client login passwords stored in its internet trading system.	Customers should develop an encryption management mechanism to encrypt the storage and transmission of sensitive data. As a CSP, in order to protect the security of data processing on the cloud for customers, HUAWEI CLOUD provides layer-by-layer protection for all stages of the data life cycle including data storage and data transmission: **(1)Data storage**: Currently, **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which supports data security on the cloud. **(2)Data transmission**: When customers provide Web site services through the Internet, they can use the certificate management service provided by HUAWEI CLOUD in conjunction with world-renowned certificate service providers. By applying and configuring a certificate for the Web site, the trusted identity authentication of the website and the secure transmission based on the encryption protocol are realized. For customer business hybrid cloud deployment and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			global layout scenarios, the **Virtual Private Network (VPN)**, **Direct Connect(DC)**, **Cloud Connection(CC)** and other services provided by HUAWEI CLOUD can be used to achieve business interconnection and data transmission security between different regions.

6.2 Infrastructure security management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.1	Deploy a Secure Network Infrastructure	A licensed or registered person should deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (DMZ) with multi-tiered firewalls, to protect critical systems (eg, internet trading system and settlement system) and client data against cyber-attacks.	Customers should develop appropriate network isolation measures to deploy network infrastructure to protect critical systems and customer data from cyber attacks. To cooperate with customers to meet regulatory requirements: **(1)**Customers can use the **Virtual Private Cloud (VPC)** to realize network isolation between different regions. The VPC service can create a private network environment for users, and realize complete isolation of different users in a three-tier network. Users have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation. **(2)**HUAWEI CLOUD's **Web Application Firewall (WAF)** is an advanced web application firewall service featuring a series of targeted optimization algorithms that give full play to Huawei's extensive experience in network attacks and defense mechanisms. HUAWEI CLOUD's WAF runs on the dual-engine architecture of regular expression rule and semantic analysis to realize high-performance protection against SQL injections, cross-site scripting (XSS) attacks, command and code injections, directory traversals, scanners, malicious bots, web shells, and CC attacks. HUAWEI CLOUD's WAF provides a user-

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			friendly and centralized management interface on which users can configure protection settings based on their service and business requirements, view WAF logs, and resolve false positive events. **(3)**HUAWEI CLOUD is built upon a solid, multi-layered full stack security framework with comprehensive perimeter defense. For example, layers of firewalls isolate networks by security zone, anti-DDoS quickly detects and protects against DDoS attacks, WAF detects and fends off web attacks close to real time, and IDS/IPS detects and blocks network attacks from the Internet in the real time while also monitoring for behavioral anomalies on the host.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2	User Access Management	A licensed or registered person should have policies and procedures in place to ensure that system access or the use of the systems are granted to users on a need-to-have basis. In addition, a licensed or registered person should review, at least on a yearly basis, the user access list of critical systems (eg, internet trading systems and settlement systems) and databases (eg, client data) to ensure that access to or use of the systems remain restricted to persons approved to use them on a need-to-have basis.	Customers should develop user account and authority management mechanism to realize that employees' access and use of the system are reasonably authorized, and the account and authority of key systems and databases should be reviewed annually. To cooperate with customers to meet regulatory requirements: **(1)**Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Except for support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the user 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. **(2)**To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 realize fully process management from user creation, authorization, authentication to rights recovery. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to realize that personnel with different responsibilities in different positions can only access the equipment under their role.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.4	Patch Management	A licensed or registered person should monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing.	Customers should develop a patch management mechanism, monitor the release of software providers' patches continuously, conduct impact assessment and testing on the patches, and install the patches in a timely manner after completing the testing. As a CSP, HUAWEI CLOUD's professional security team performs security hardening on public images and patches any system vulnerabilities that may occur. Secure, updated public images are created with the help of an image factory and provided to users through **Identity and Access Management (IAM)**. Pertinent hardening and patch information is also provided to users for reference during image testing, troubleshooting, and other O&M activities. When creating VMs, users can decide based on their applications and security policies whether to use an up to-date public image or create a private image that has the required security patches installed.
2.5	End-point Protection	A licensed or registered person should implement and update anti-virus and anti-malware solutions (including the corresponding definition and signature files) on a timely basis to detect malicious applications and malware on critical system servers and workstations.	Customers should develop anti-virus management mechanisms, implement and update anti-virus solutions. Customers can use the HUAWEI CLOUD **Host Security Service (HSS)**to protect host security. HSS provides asset management, vulnerability management, baseline check, and malicious program detection functions to help customers better manage host security risks, detect and prevent hacker intrusion in real time

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.7	Physical Security	A licensed or registered person should establish physical security policies and procedures to protect critical system components (eg, system servers and network devices) in a secure environment and to prevent unauthorized physical access to the facilities hosting the internet trading system as well as the critical system components.	Customers should develop physical security management policies and procedures to prevent personnel from accessing critical system infrastructure without authorization. To cooperate with customers to meet regulatory requirements, 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, during the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to improve the physical security and environmental safety of HUAWEI CLOUD data centers. See section 5.1 Physical and Environmental Security of ***HUAWEI CLOUD***

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Security White Paper for more information.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.8	System and Data Backup	A licensed or registered person should back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis. A licensed or registered person should also adopt an appropriate recovery method to enable successful roll-back of major system changes.	Customers should develop a backup management mechanism, regularly back up important data and files, and adopt appropriate backup and recovery plans to successfully roll back major system changes. To cooperate with customers to meet regulatory requirements: **(1)**HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of **Object Storage Service (OBS)**, **Volume Backup Service (VBS)**, and **Cloud Server Backup Service (CSBS)** to back up include 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 realize that data will not be lost in the event of a disaster. **(2)**Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to improve 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			fails, it can also balance traffic load to other centers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.9	Contingency Planning for Cybersecurity Scenarios	In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, a licensed or registered person should make all reasonable efforts to cover possible cyber-attack scenarios such as distributed denial-of-service (DDoS) attacks and total loss of business records and client data resulting from cyber-attacks (eg, ransomware) in the contingency plan and crisis management procedures.	Customers should develop a security incident response mechanism, and develop a business continuity plan and crisis management procedures for responding to cyber-attacks. To cooperate with customers to meet regulatory requirements: **(1)**HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices. Incidents will be ranked based on the extent to which security incidents affect the customer's business, and will initiate a customer notification process to notify customers of the incident. After the event is resolved, an event report will be provided to the customer. **(2)** HUAWEI CLOUD has formulated various specific contingency plans to deal with complex security risks in the cloud environment. Each year, HUAWEI CLOUD conducts contingency plan drills for major security risk scenarios to quickly reduce potential security risks and ensure cyber resilience when such security incidents occur.

6.3 Cybersecurity management and supervision

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.2	Cybersecurity Incident Reporting	A licensed or registered person should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (eg, to the responsible officer(s) or executive officer(s) in charge of internet trading) and externally (eg, to clients, the SFC and other enforcement bodies, where appropriate).	Customers should develop a security incident escalation mechanism, define all kinds of security incidents reporting methods and reporting objects clearly. To meet regulatory requirements with our customers, HUAWEI CLOUD has developed a complete process for event management and notification. If an event occurs on the HUAWEI CLOUD Base Platform, relevant personnel will analyze the impact of the event according to the process. If the event has or will have an impact on the cloud service customers, HUAWEI CLOUD will start to notify customers of the event. The contents of the notice include but not limited to description of the event, the cause, impact, measures taken by HUAWEI CLOUD, and measures recommended for customers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.3	Cybersecurity Awareness Training for Internal System Users	A licensed or registered person should provide adequate cybersecurity awareness training to all internal system users at least on a yearly basis. When designing the content of the training programme, the licensed or registered person should take into account the type and level of cybersecurity risks it faces.	Customers should establish a cybersecurity training mechanism, provide adequate and regular security awareness training for all employees, As a CSP, to improve cybersecurity awareness in company-wide, avoid non-compliance risks and realize normal business operations, Huawei provides employee security awareness training in three ways: company-wide awareness training, awareness promotion events, and the signing of Business Conduct Guidelines (BCG) commitment agreements. By utilizing industry best practices, Huawei has established a comprehensive cybersecurity training program, which implements security competency trainings for new hires as well as existing and newly-promoted employees. This program boosts employees' security competencies and improves employee capabilities of delivering to our customers secure products, services, and solutions that are compliant with all relevant laws and regulations. In order to streamline internal management and to minimize any potential impact of personnel management on our business continuity and security, HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers. This program includes: on boarding security review, on the job security training, on boarding qualifications management, off boarding security review. See section 4.4 Human Resource Management of ***HUAWEI CLOUD Security White Paper*** for more information.

7 How HUAWEI CLOUD Meets and Assists Customers to Meets the Requirements of SFC Good industry practices for IT risk management and cybersecurity

SFC released *Good industry practices for IT risk management and cybersecurity* on October 27, 2017. This policy sets LCs' IT risk and cybersecurity management requirements from secure system and network infrastructure, system access control and data protection, security monitoring and capacity management, system development and change management, data backup and contingency planning, vendor management and raising cybersecurity awareness of internal system users and other domains.

When LCs are seeking to comply with the requirements provided in *Good industry practices for IT risk management and cybersecurity*, HUAWEI CLOUD, as a CSP, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to CSPs in *Good industry practices for IT risk management and cybersecurity*, and explains how HUAWEI CLOUD, as a CSP, can help LCs to meet these requirements.

7.1 Secure system and network infrastructure

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
B1	Network Isolation	Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. In particular, control and protect sensitive data traffic between different network segments.	Customers should segment the network and provide access control over data or system connections in different regions. Customers can use the **Virtual Private Cloud (VPC)** to realize network isolation between different regions. The VPC service provided by HUAWEI CLOUD for customers can create a private network environment for users, and realize complete isolation of different users in a three-tier network. Users have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
B2-B4	Network Infrastructure Security	B2.Set up the Demilitarised Zone (DMZ) with robust security controls by: - Deploying multi-tiered firewalls of different brands and types to control and filter network traffic between the DMZ and the trusted internal networks; - Implementing Intrusion Prevention System, Web Application Firewall, anti-APT (Advanced Persistent Threat) solutions to protect the internet-facing servers in the DMZ; - Deploying Intrusion Detection System (IDS) and System Information & Event Management (SIEM) solutions to detect and monitor unauthorized access and data transfer; - Not storing or caching sensitive data such as customer login credentials within the DMZ; and - Protecting sensitive data	Customers should set up a DMZ, and take appropriate network security monitoring and protection measures, such as firewalls, intrusion detection systems, and Web application firewalls. As an CSP, HUAWEI CLOUD engages our business partners to provide users with cloud security consulting services and assist users in not only the security configuration of their virtual networks and virtual systems (including virtual hosts and guest virtual machines) as well as system- and DB-level security patch management, but also the configurations of virtual firewalls, API gateways, security incident response, disaster recovery, and advanced security services such as anti-DoS/DDoS protection. **(1)**HUAWEI CLOUD's **Web Application Firewall (WAF)** is an advanced web application firewall service featuring a series of targeted optimization algorithms that give full play to Huawei's extensive experience in network attacks and defense mechanisms. HUAWEI CLOUD's WAF runs on the dual-engine architecture of regular expression rule and semantic analysis to realize high-performance protection against SQL injections, cross-site scripting (XSS) attacks, command and code injections, directory traversals, scanners, malicious bots, web shells, and CC attacks. HUAWEI CLOUD's WAF provides a user-friendly and centralized management interface on which users can configure protection settings based on their service and business requirements, view WAF

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		through strong encryption during transmission within the DMZ. B3. Implement secure configuration of key IT systems, i.e. system hardening. Disable or remove any unused programs, ports, computer processes and privileged accounts. B4. Implement application whitelisting solutions to prevent installation of unauthorized applications on users' computers or servers.	logs, and resolve false positive events. **(2)** HUAWEI CLOUD's **Virtual Private Network (VPN)**service is used to establish a secure encrypted communication channel that complies with industry standards between a remote network and users VPC such that a user's existing traditional data center seamlessly extends to HUAWEI CLOUD while ensuring end-to-end data confidentiality. Currently, HUAWEI CLOUD uses IPSec VPN together with Internet Key Exchange (IKE) to encrypt the data transport channel and assist transport security. **(3)** Customers can use the HUAWEI CLOUD **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 constantly, and meet graded security protection compliance requirements. Some functions of HSS are as follows: • **Account cracking prevention:** detects password cracking attacks on accounts such as SSH, RDP, FTP, SQL Server, and MySQL, blocks the identified attack source IP addresses for 24 hours, and forbids them to log in again to prevent hosts from being intruded due to account cracking. • **Asset management:** manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			• **Baseline check:** checks system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks. • **Detection of malicious programs:** By detecting program features and behaviors and using the AI image fingerprint algorithm and cloud-based virus scanning and removal, the system can effectively identify malicious programs, such as viruses, Trojan horses, backdoors, worms, and mining software, and provide one-click isolation and virus removal capabilities.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
B5	Distributed Denial of Service(DDoS)	Assess the risk of DDoS attacks and implement anti-DDoS mechanisms and solutions by filtering high volume and suspicious incoming traffic/ cyber-attacks as appropriate.	Customers should assess the risk of DDoS attacks and implement effective anti-DDoS attack mechanisms and solutions. As a CSP, HUAWEI CLOUD provides customers with two kinds of Anti-DDoS attack services: **Anti-DDoS** and **Advanced Anti-DDoS (AAD)**. Anti-DDoS is a traffic scrubbing service that protects resources such as Elastic Cloud Server and Elastic Load Balance instances from network and application layer distributed denial-of-service (DDoS) attacks. It notifies users of detected attacks instantly, ensures bandwidth availability as well as the stable and reliable running of services. AAD can be used to protect HUAWEI CLOUD and non-HUAWEI CLOUD hosts. User can change the DNS server or external service IP address to a high-defense IP address, thereby diverting traffic to the high-defense IP address for scrubbing malicious attack traffic. This mechanism assists that important services are not interrupted. HUAWEI CLOUD Anti-DDoS attack services provide fine-grained DDoS mitigation capabilities to deal with the likes of Challenge Collapsar attacks and ping, SYN, UDP, HTTP, and DNS floods. Once a protection threshold is configured (based on the leased bandwidth and the business model), Anti-DDoS will notify the affected user and activate protection in the event of a DDoS attack. HUAWEI CLOUD Anti-DDoS attack services also leverages other HUAWEI CLOUD technologies to enhance its security capabilities: namely, the secure infrastructure and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			platform, secure network architecture and perimeter protection, virtual network isolation, API security, and log auditing.

7.2 System access control and data protection

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
C1&C2&C5	System Access Control	C1. Establish formal access management and privileged account management procedures with adequate checks and balances. Control, record and monitor all access to end point devices, servers and network equipment using privileged or emergency accounts. Implement Identity Access Management (IAM) and Privileged Access Management (PAM) tools to help ensure the consistent implementation of access management practices. C2. Limit privileged user access to operating systems to prevent installation of malicious applications, unauthorized manipulation of system configurations or removal of security tools on	Customers should establish access control and privileged account management procedures to monitor, record, and audit access to terminals, servers, and network devices. At the same time, restrict the use of privileged accounts to avoid illegal operations using privileged accounts. As an CSP, **(1)**HUAWEI CLOUD's unified **Identity and Access Management (IAM)** provides cloud resource access control for customers. With IAM, the customer administrator can manage user accounts and control the access privileges of these user accounts. When multi-user cooperative operation resources exists in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and assist the security of user accounts by setting a login authentication strategy, password strategy and access control list. Through the above measures, we can effectively control privileges and provide emergency accounts. Customers can also use the **Cloud Trace Service (CTS)** as a supplement to provide operational records of cloud service resources for users to query, and for audit. **(2)**When HUAWEI CLOUD operators access the HUAWEI CLOUD management network for centralized management of the system, they need to use the only identifiable employee

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		users' computers or servers. C5. Do not allow system development personnel (including vendors) to have access to the production environment without prior written senior management's approval, supported by explanation. Where access to the production environment is allowed, put in place a mechanism to record and monitor such activities.	identity account. User accounts are equipped with strong password security policies, and passwords are changed regularly to prevent brute-force cracking. Two-factor authentication (2FA) is also used to authenticate cloud personnel, such as with a USB key, smart card and so on. Employee accounts are also used to log on to the VPN and access gateway to further contain user logins for auditing.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
C3-C4	Key Management	C3. Establish formal cryptographic key management policy and procedures to govern the life cycle of cryptographic keys for the encryption of confidential and sensitive data. C4. Implement data protection controls by adopting system login passwords that are salted and one-way hashed, preferably with a slow hash function.	Customers should establish password management policies and procedures, use secure encryption algorithms to encrypt confidential and sensitive data, and manage the life cycle of keys effectively. In order to cooperate with customers to meet regulatory requirements, HUAWEI CLOUD provides **Data Encryption Workshop (DEW)**, which is a comprehensive cloud data encryption service. It provides functions such as dedicated encryption, key management, and key pair management. With dedicated encryption service, users can select the hardware encryption machine certified by the OSCCA or FIPS 140-2 Level 3 to achieve high-performance and user-exclusive encryption capabilities. DEW supports SM1 to SM4 key encryption algorithms developed in China. Through the key management function which provides full-lifecycle key management. Except the customer, nobody can obtain keys to decrypt data without authorization, to protect the data security on the cloud. DEW adopts the layered key management mechanism. Hardware security module (HSM) adopted by HUAWEI CLOUD 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

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

7.3 security monitoring and capacity management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
D2&D5	Security Monitoring and Log Management	D2. Tailor behavioral monitoring solutions and their underlying parameters to enable detection of malicious activities (e.g. monitoring the data exfiltration over certain types of information, such as customer identifiers, source codes and large volume of encrypted files, after normal office hours) by taking into consideration different types of cyber-attacks. D5. Maintain and review audit trail records / access logs for computers or network systems to identify any unauthorized access attempts or system security attacks.	Customers should take network security monitoring measures to detect malicious activities, keep and audit the computer and network system access and operation records. To cooperate with customers to meet regulatory requirements: **(1)**HUAWEI CLOUD is built upon a solid, multi-layered full stack security framework with comprehensive perimeter defense. For example, layers of firewalls isolate networks by security zone, anti-DDoS quickly detects and protects against DDoS attacks, WAF detects and fends off web attacks close to real time, and IDS/IPS detects and blocks network attacks from the Internet in the real time while also monitoring for behavioral anomalies on the host. Given that a public cloud usually needs to process huge amounts of traffic while also exposed to a wide variety of attacks, HUAWEI CLOUD employs its situation awareness analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to rapid and thorough detection of ongoing attacks and forecast potential threats. **(2)** 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/ resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. HUAWEI CLOUD also has a dedicated internal audit department that performs periodic audits on O&M activities. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
D7-D8	Performance and Capacity Management	D7. Establish performance alert thresholds, for example, CPU usage, memory usage, disk I/O and free space, bandwidth to facilitate monitoring of system and network activities. D8. Implement alert mechanism to timely notify the relevant parties for corrective actions when approaching performance alert thresholds.	Customers should establish performance and capacity management mechanisms, set system performance thresholds, and conduct continuous monitoring and abnormal response. In order to cooperate with customers to meet regulatory 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 user cloud service. At the same time, **Cloud Eye Service (CES)** provides users with a robust monitoring platform for **Elastic Cloud Server (ECS)**, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.

7.4 system development and change management

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
E1	Change Management	Establish formal change management procedures and implement effective controls over system modification, production deployment and system fall-back. In particular, obtain written management approval for both scheduled and emergency changes/fixes.	The customer should develop a change management procedure, take effective monitoring measures for system changes, and require that any changes must be reasonably authorized before they can be implemented. HUAWEI CLOUD, as CSP, is responsible for the management of the infrastructure it provides and the various cloud services of IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a comprehensive change management process and regularly reviews and updates it. Define the change category and change window, as well as the change notice mechanism, depending on the extent to which the change may affect the business. The process requires that all change requests be submitted to the HUAWEI CLOUD change committee after the change manager makes a judgment. After the review, the network can be changed according to the plan. All changes need to be fully validated before application with tests such as production environment tests, gray release tests, and blue-green deployment. This make that the change committee has a clear understanding of the change, the timeframe, the possible rollback of the change, and all possible impacts.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
E2	Develop Security Management	Mandate the following security practices in the software development life cycle (SDLC) to allow early identification and remediation of security vulnerabilities prior to the launch of new systems or major system changes: - Consider security requirements (e.g. user authentication and authorization, session management, data integrity, audit logging) during the system design phase; - Establish secure programming practices; - Conduct source code review including peer review and automated source code scanning; and - Conduct security testing prior to migration to production environment.	Customers should establish a development safety management mechanism to manage the software development life cycle, including security requirements analysis, security design, security coding, code review, security testing, etc. As a CSP, 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. Details as follows: **(1)**HUAWEI CLOUD and related cloud services comply with the security and privacy design principles and norms, applicable laws and regulations. Threats are analyzed according to business scenarios, data flow diagrams and networking models in the security requirements analysis and design phase. When a threat is identified, the design engineer will formulate mitigation measures according to the reduction library and the safety design library and complete the corresponding safety design. All threat mitigation measures will eventually be converted into security requirements and security functions, and according to the company's test case library, will be used to complete the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			design of security test cases, ensure the safety of products and services. **(2)**HUAWEI CLOUD strictly complies with the security coding specifications of various programming languages issued by Huawei. Static code analysis tools are used for routine checks, and the resulting data is entered in the cloud service tool chain to evaluate the quality of coding. Before all cloud services are released, static code analysis alarms must be cleared to effectively reduce the security issues related to coding when online. **(3)**HUAWEI CLOUD takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services to make that the released cloud services meet security requirements. Testing is conducted in a test environment which is isolated from the production environment, and production data shall be avoided from being tested. If production data is used for testing, it must be desensitized, and data cleaning is required after use.

7.5 Cybersecurity risk assessment, Cyber-attack simulation and incident response

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
F1-F3	Cybersecurity Risk Assessment, Cyber-attack Simulation and Incident Response	F1. Carry out simulations of real-life cyber-attack scenarios and the latest trends of cyber-attacks to validate the effectiveness of the cyber defense mechanisms. F2. Conduct regular independent assessments of Internet-facing and internal systems and underlying technology infrastructure, people and processes by qualified professionals who are independent of the system development and maintenance functions. F3. Arrange post-mortem review to be performed by independent functions or external professionals in the event of material security incidents, including system delays and system failures.	Customers should establish a cybersecurity management mechanism, implement cybersecurity assessments, cyber-attack simulation, and security incident response measures. To meet customer compliance requirements, **(1)**HUAWEI CLOUD regularly conducts internal cyber security practical exercises (such as Red team vs Blue team) and penetration testing and security assessment performed by third party with regular monitoring, checks, and removal of any security threats so as to protect the security of the cloud services. **(2)**The Huawei Product Security Incident Response Team (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 realize 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 users' 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, and response and disclosure

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			mechanism. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and realize 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.

7.6 Data backup and contingency planning

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
G1-G4	Data Backup and Contingency Planning	G1. Encrypt all backup media containing confidential and sensitive data and where applicable protect such media physically (e.g. use of locked box for storage transportation) to ensure secure storage and transportation between locations. G2. Perform restoration test of data backup on a regular basis to ensure effectiveness of data recovery. G3. Establish a disaster recovery/ secondary site to continue internet trading services or make alternative arrangements in the event of primary site outage with a view to minimizing disruption of internet trading services provided to clients. G4. Conduct disaster recovery drill at least annually and update the disaster recovery	Customers should establish a backup management mechanism to back up confidential and sensitive data, properly keep the backup storage media and conduct regular backup recovery tests. In addition, a disaster recovery plan should be developed, tested and updated regularly. To cooperate with customers to meet regulatory requirements: **(1)**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. To improve the emergency response capability, customers can perform the recovery drill periodically. The Backup and Archive solution allows customers to use backups to restore data in the in-cloud system. After the data is restored, resources can be released, significantly reducing the recovery drill cost. **(2)**Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		plan where appropriate.	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. In addition to providing high-availability infrastructure, redundant data backup centers, and disaster preparedness in available areas, HUAWEI CLOUD has also developed business continuity plans and disaster recovery plans that are regularly tested to realize that the emergency plan is in line with the current organizational and IT environment. If HUAWEI CLOUD is required to assist in performing the customer's disaster recovery drills, HUAWEI CLOUD will actively cooperate.

7.7 Vendor management – onboarding and ongoing audit

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
H1-H3	Vendor Management – Onboarding and Ongoing Audit	H1. Evaluate the cybersecurity resiliency of prospective vendors before onboarding. H2. Include in the service level agreement with vendors (and/or intra-group entities) the following cybersecurity requirements, among others: - compliance with company cybersecurity policies; - escalation of security incidents; - removal/ destruction of data stored at vendors' systems and backups in the event of contract termination or deemed necessary; and - reasonable indemnification or liability provisions. H3. Conduct cybersecurity risk assessment and on-site audit of vendors, or review of auditor report of vendors, on a	Customers should evaluate the supplier's cyber security capabilities before establishing business relationships, and incorporate cyber security requirements into the service agreement signed with the supplier. As a CSP: **(1)**Every HUAWEI CLOUD data center has numerous nodes and complex functional zones. To simplify its network security design, prevent the propagation of network attacks in HUAWEI CLOUD and minimize the potential impact of attacks, HUAWEI CLOUD defines both security zones and service planes, and implements a network segregation strategy in HUAWEI CLOUD by referencing and adopting the security zoning principle of ITUE.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. HUAWEI CLOUD always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, HUAWEI CLOUD has adopted a set of network security mechanisms to enforce stringent controls and assist cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks, which will be covered in more detail throughout the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		regular basis and require vendors to take remedial actions upon the identification of material deficiencies.	rest of this chapter and the following chapters of the white paper. **(2)**HUAWEI CLOUD provides online version of ***HUAWEI CLOUD Customer Agreement*** and ***HUAWEI CLOUD Service Level Agreement*****,** which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customer auditing and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the actual situation. **(3)**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 has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. HUAWEI CLOUD is regularly audited by professional third-party auditors on annual basis and provides special assistance to respond positively to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and cooperate with audit activities initiated by customers.

7.8 Raising cybersecurity awareness of internal system users

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
I1-I2	Raising Cybersecurity Awareness of Internal System Users	I1. Provide structured cybersecurity awareness training to internal system users, including regular courses for new joiners, refresher courses and ad-hoc courses on a needs basis, e.g. upon becoming aware of sudden cybersecurity threats, explaining the company's cybersecurity-related policies and procedures and providing practical guidance to staff on how to implement these policies and procedures. I2. Evaluate staff's understanding and compliance with company policies on IT risk and cybersecurity on a regular basis, with short tests, reminder prompts (e.g. not to open links and attachments in any suspicious emails to prevent against ransomware attack) and phishing attack	Customers should establish a cybersecurity training mechanism, provide adequate and regular security awareness training for all employees. As a cloud service provider, to improve cybersecurity awareness in company-wide, avoid non-compliance risks, and improve normal business operations, Huawei provides employee security awareness training in three ways: company-wide awareness training, awareness promotion events, and the signing of Business Conduct Guidelines (BCG) commitment agreements. By utilizing industry best practices, Huawei has established a comprehensive cybersecurity training program, which implements security competency trainings for new hires as well as existing and newly-promoted employees. This program boosts employees' security competencies and improves employee capabilities of delivering to our customers secure products, services, and solutions that are compliant with all relevant laws and regulations. In order to streamline internal management and to minimize any potential impact of personnel management on our business continuity and security, HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers. This program includes: on boarding security review, on-job security training, on boarding qualifications management, off boarding security review.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		simulation as part of evaluation process.	See section 4.4 Human Resource Management of ***HUAWEI CLOUD Security White Paper*** for more information.

8 Conclusion

This whitepaper describes how HUAWEI CLOUD provides cloud services that follow the regulatory requirements of securities and futures industry in Hong Kong SAR, China and shows that HUAWEI CLOUD complies with key regulatory requirements issued by SFC in Hong Kong SAR, China. This aims to help customers learn more about HUAWEI CLOUD's compliance status with regulatory requirements related to securities and futures industry in Hong Kong SAR, China, and to assure customers that they can store and process 'their 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 securities and futures industry in Hong Kong SAR, China on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This whitepaper is for general reference only and does not have any legal effect or constitute any legal advice. Customers should assess their own use of cloud services as appropriate and be responsible for ensuring compliance with relevant regulatory requirements from securities and futures industry in Hong Kong SAR, China when using HUAWEI CLOUD.

9 Version History

Date	Version	Description
2020-09-30	1.0	First release

