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

Issue 1.0

Date 2022-05-16

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Background and Purpose

Following the recent wave of technological development, more and more Financial Institutions (FIs) are planning to transform their business by leveraging high-technology to reduce costs, improve operational efficiency and innovate. To regulate the application of Information Technology (IT) in the financial industry, Mexico's Ministry of Finance and Public Credit (SHCP), National Banking and Securities Commission (CNBV) and the Bank of Mexico (Banxico) have issued a series of regulatory laws and general provisions, setting out requirements on cybersecurity and technology outsourcing management of Mexican FIs.

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

1.2 Introduction of Applicable Financial Regulatory Requirements in Mexico

Currently, the regulatory entities of the Mexican FIs mainly include the Bank of Mexico (Banxico), the Ministry of Finance and Public Credit (SHCP) and its six subordinate departments.

The Bank of Mexico (Banxico): The Central Bank of Mexico, the most important institution in the Mexican financial system and is the supervisor and controller of all banks in Mexico.

The Ministry of Finance and Public Credit (SHCP): A centralized government agency in Mexico whose head is appointed by the President of Mexico. Its governmental functions are aimed at obtaining monetary resources from various sources to finance the development of the country.

The National Banking and Securities Commission (CNBV): A branch of the SHCP that has technical autonomy and executive authority, it is responsible for

supervising and managing Mexican financial institutions within the scope of its authority, maintaining and promoting the stable development of the Mexican financial system and protecting public interests.

The National Insurance and Bonding Commission (CNSF): A branch of SHCP that oversees compliance with the relevant regulatory framework in Mexico's insurance and guaranty industries and helps to extend services to as many people as possible.

Banxico, SHCP and CNBV have jointly issued the following credit, fintech and securities laws and related general regulations to regulate industry compliance management and supervision:

- **Credit Institutions Law and its General Provision:** Including the Credit Institutions Law and the General Provisions of the Credit Institutions Law.
- **Financial Technology Institutions Regulatory Law (Fintech Law) and its General Provision:** Including the Financial Technology Institutions Regulatory Law, the Secondary Regulatory Requirements of the Financial Technology Institutions Regulatory Law, and the General Provisions of the Financial Technology Institutions Regulatory Law.
- **The Securities Market Law and its General Provisions:** Including the Securities Market Law, the General Provisions Applicable to Stock Exchanges, the General Provisions Applicable to Brokerage Companies, and the General Provisions Applicable to Securities Depository Institutions.

Banxico, SHCP, and CNSF jointly issued regulatory laws and related general regulations for the insurance and guaranty industry to regulate industry compliance management and supervision:

- **The Insurance and Guarantee Institution Law and its General Provisions**: The Insurance and Guarantee Institution Law and the General Provisions Applicable to the Insurance and Guarantee Institution Law.

1.3 Basic Definitions

- **HUAWEI CLOUD**

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

  Registered users having a business relationship with HUAWEI CLOUD.
- **ITF:**

  Fintech institutions, i.e. financiers and electronic payment fund institutions.
- **Technical Infrastructure:**

  Operating systems, databases, software and applications used by ITF, companies authorized to work with new models and financial entities to support operations.

2 HUAWEI CLOUD's Certification

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

Certification	Description
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
CSA-STAR Gold Certification	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL3+ 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.
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.

Certification	Description
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data Protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow and personnel management of the 3D protocol execution environment.

Regional standard certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	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.
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.

Certification	Description
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) (China)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. HUAWEI private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS (China)	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification - Cyberspace Administration of China (CAC) (China)	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.
Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
OSPAR certification (Singapore)	OSPAR is an audit report issued by the Association of Banks in Singapore (ABS) to outsourcing service providers. HUAWEI CLOUD passed the guidelines (ABS Guidelines) of the Association of Banks of Singapore (ABS) on controlling the objectives and processes of outsourcing service providers, proving that HUAWEI CLOUD is an outsourcing service provider that complies with the control measures specified in the ABS Guidelines.

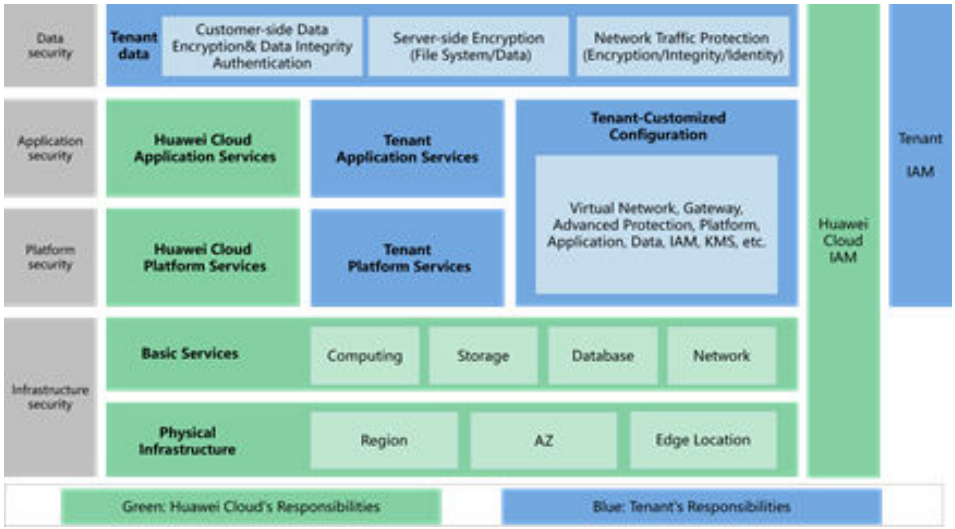
Certification	Description
TISAX (Europe)	TISAX (Trusted Information Security Assessment Exchange) is a security standard for information security assessment and data exchange in the automotive industry launched by the Verband der Automobilindustrie (VDA) and the European Automobile Industry Security Data Exchange Association (ENX). The passing of the TISAX indicates that HUAWEI Cloud has met the European-recognized information security standards for the automotive industry.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance certificate, please refer to the official website of HUAWEI CLOUD "**Trust Center -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 tenant and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenants to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the tenant and HUAWEI CLOUD:

Figure 3-1 Responsibility Sharing Model



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

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

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

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

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

4 HUAWEI CLOUD Global Infrastructure

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

5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Credit Institutions Law and its General Provision

The Credit Institutions Law and its General Provision describe CNBV's supervision and recommendations on activities when Mexican financial institutions choose to use cloud services, as well as the matters to be handled by financial institutions. The Credit Institutions Law is a directive with legal force and is a high-level management requirement. The General Provisions of the Credit Institutions Law is a guide to the implementation of the Credit Institutions Law.

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

5.1 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Credit Institutions Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
46.2.1	Section I: General Rules	FIs must comply with the following regulations when signing outsourced business service contracts with third parties: 1. Comply with the technical and operational guidelines relating to the services provided, as well as the relevant provisions guaranteeing the confidentiality of the information of the users of the banking system in the provision of the services. 2. FIs shall establish requirements for control procedures when third parties provide services. 3. FIs shall establish procedures and policies to monitor third parties' performance of contracts, which shall include the obligation of third parties to provide records, information and technical support related to the services as requested by the CNBV Commission and the institution's external auditors. 4. The CNBV Commission and FIs have the right to audit, supervise and monitor third-party service providers at any time, and the FIs have the obligation to provide relevant reports to the CNBV Commission.	FIs should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. HUAWEI CLOUD provides the **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		The CNBV Commission may issue an opinion or corrective action to the financial institution based on the results of an audit of third party. 5. Employees of third parties, as well as ex-employees, shall also comply with the provisions of this Article. 6. The third party shall cooperate with the financial institution to select other outsourced service providers to jointly provide the services. 7. If FIs fail to comply with this provision, the CNBV Commission may, after the institution has been granted the right to a hearing, order partial or total, temporary or final suspension of services or commissions provided through the third party concerned.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
46.2.2	Section I: General Rules	1. If FIs enter into an outsourced service with a third party, it shall not relieve the financial institution or its directors and employees of the obligation to comply with the provisions of this Law and regulations and relevant general provisions. 2. The CNBV Commission, through FIs, may request the outsourced service provider to provide information related to its services, including books, records and documents.	FIs may contract outsourcing services with third parties, but cannot outsource legal liabilities. FIs or their directors and employees shall bear corresponding responsibilities in accordance with the requirements of this Law. The financial institution shall cooperate with the CNBV Commission to collect relevant information from the financial institution's outsourced service providers. HUAWEI CLOUD will assign dedicated personnel to actively respond to the requirements of FIs and provide related materials.
126	Separate Section: Inspection and Supervision	FIs are obligated to provide the CNBV Commission with the support required for inspection and supervision, including: 1. Provide data, reports, records, documents, correspondence and other required documents. 2. Guarantee the CNBV Commission access to its office premises and other facilities for inspection.	FIs should cooperate with the CNBV Commission's inspections. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with FIs or the CNBV Commission in the audit.

5.2 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions of the Credit Institutions Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
318	Section I: General Provisions	FIs should comply with the following requirements when signing service contracts with third parties: 1. Provide a report on the criteria and policies for selecting third-party service providers. 2. Specify in the service contract or in a document unconditionally accepted by a third party: a. Access to the physical premises of the outsourced service provider by the receiving institution's external auditors, by the CNBV Commission, or by a third party designated by the CNBV Commission itself, to verify that the services or entrustments provided by the institution allow the financial institution to comply with the legal requirements applicable to it. The financial institution may appoint a representative to accompany the visit. b. The receiving institution audits the services or commissions agreed upon in the above-mentioned contract to	FIs should include the requirements in their contracts with third parties. FIs should establish criteria for the selection of third-party service providers and mechanisms for monitoring third-party performance and contract performance. HUAWEI CLOUD provides the **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		verify compliance with the regulations applicable to the institution. c. Provide systems, records, manuals and documents related to the services to the institution's external auditors and the CNBV Commission or its designated third party, upon request by the institution. d. Notify the financial institution at least 30 calendar days in advance of any change in the corporate purpose or internal organization of the third party service provider that may affect the provision of the services covered by the contract. 3. Policies and procedures exist to monitor third party performance and contract performance. Such policies and procedures should include the following related matters: a. Limit the possibility of subcontracting services by third parties. b. Confidentiality and security of financial institution information. c. Obligations of the institution and third parties, procedures for monitoring third parties' compliance with the Contract, and possible legal	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		consequences of non-compliance. d. Mechanisms for the settlement of disputes relating to service contracts. e. Business continuity plans, including emergency response procedures in the event of disasters. f. Establish guidelines to ensure that third parties receive information on a regular basis in relation to the services contracted. g. If the service or commission to be contracted involves the use of technology or telecommunications infrastructure, the minimum security guidelines set out in this Regulation shall be observed. 4. Audits are conducted every two years to verify compliance with the provisions of this chapter and, where applicable, minimum safety guidelines and report the results of the audit to the Board of Directors and the Audit Committee. 5. To provide that the general manager, the Audit Committee and the institution's internal auditors, in accordance with their authority, supervise the technology, information processing infrastructure and	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		information processing, control and security mechanisms used by outsourced service providers to provide services. 6. Develop guidelines that allow FIs to evaluate contracts to identify circumstances that may impact an institution's business, including: a. The organization has the ability to maintain business continuity in the event of an emergency. b. The complexity and time required to find a third party to replace the original contracting party. c. Restrictions on making decisions that have a significant impact on the administrative, financial, operational or legal situation of the institution itself. d. Notify the institution at least 30 calendar days in advance of any change in its corporate purpose or internal organization that may affect the provision of the services agreed upon as a contract. e. The impact the suspension may have on the institution's finances, reputations and operations. f. Vulnerability of financial institution information.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		7. The general manager of the financial institution shall be responsible for approving the selection policies and criteria for third-party service providers.	
326	Section III: Service or Entrustment Contracts with Third Parties	When FIs sign a service contract with a third party, it shall explain to the CNBV Commission the minimum security standards agreed with the third party before signing the contract, and send the minimum security standards to the CNBV Commission at least 20 working days before signing the contract. The financial institution shall obtain the approval of the CNBV Commission before carrying out the outsourced services.	FIs shall submit to the CNBV Commission for approval at least 20 working days before it plans to enter into a service contract with a third party, stating the type of business to be carried out using the third party's services and how to comply with the minimum security guidelines required by these general provisions. HUAWEI CLOUD will cooperate with FIs to provide related reporting materials. In addition, HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy of HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key information security directions and objectives, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
327	Section III: Service or Entrustment Contracts with Third Parties	The notice referred to in No. 326 shall be signed by the general head of the financial institution and, if the service involves the use of technology or telecommunications infrastructure, the notice shall also contain a technical report specifying the type of banking business or services carried out using the technology infrastructure provided by third parties and compliance with minimum security guidelines for the procurement of services under this provision.	vendor management, information security incident management, and business continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
328	Section III: Service or Entrustment Contracts with Third Parties	If the services provided by third parties are partly or wholly provided or performed outside the national territory or by residents abroad, the financial institution shall, at least 20 working days before the conclusion of the contract, apply to the Vice-President of the CNBV Commission responsible for supervision for the relevant authorization and submit the following documents: 1. Information about the country in which the third party or entrusted agent with whom the contract is concluded resides, the protection measures provided by its domestic law for personal data, or the country of residence has entered into an international agreement with Mexico on such matters. 2. Institution must declare to the CNBV Commission that they will maintain at least the documents and information relating to evaluations, audit findings and performance reports at their principal offices located in the United Mexican States. Similarly, when requested by the CNBV Commission, Spanish-language versions of such documents shall be provided. 3. The financial institution states in the agreement that the signing of a service or entrustment	FIs should establish contracts with third parties in accordance with relevant requirements. When FIs enter into an outsourced service contract with an institution outside Mexico or with a resident outside Mexico, it shall apply to and obtain authorization from the CNBV Commission 20 working days prior to the conclusion of the contract. When applying to the CNBV Commission, FIs shall provide the relevant documents as required by these general provisions. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with FIs in providing related materials.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		contract will not affect the institution's compliance with this provision and is approved by the Board of Directors and the Audit Committee.	
330	Section IV: Final provisions	1. FIs shall at all times be responsible for services provided by third parties authorized by it and for non-compliance by third parties. 2. This provision shall not affect civil, administrative or criminal liability that may be incurred by third parties or entrusted agents or their employees for violations of the provisions of applicable law. 3. Similarly, this provision shall be established in contracts concluded between the institution and third parties or entrusted agents.	FIs should establish contracts with third parties in accordance with relevant requirements. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. For example, the contract specifies the responsibilities of both parties under this Law.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
332	Section IV: Final provisions	When the CNBV Commission believes that an institution's financial stability, business continuity, or protection of the public interest may be affected, or the institution fails to comply with this and other applicable provisions, the CNBV Commission may, after the institution has been granted the right to a hearing, Order the partial or total, temporary or final suspension of services or commissions provided through the third party concerned. Unless, in the exercise of the hearing right, the financial institution submits a formalization plan for review by the CNBV Commission, which makes an appropriate decision within 30 calendar days.	When the CNBV Commission considers that the financial institution does not meet the requirements of this general provisions, the financial institution shall cooperate in submitting a standardized solution to the CNBV Commission for review and suspend the contract with the relevant third party if necessary. HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with FIs in providing related materials.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
333	Section IV: Final provisions	1. The institution shall maintain a list containing the type and characteristics of contracted services and businesses, as well as information on service providers or entrusted agents, and distinguishing between persons residing within or outside the country. 2. The institution shall indicate in the list referred to in this Article its authorized service provider or entrusted agent and, if necessary, provide the list to the CNBV Commission for review. 3. Without prejudice to the foregoing, the institution shall submit to the CNBV Commission, within 90 calendar days after the end of the fiscal year, an annual report detailing the results of the review conducted by the institution in accordance with the procedures established by it.	FIs should develop and maintain a list of their suppliers, which should include basic information about the service provider, such as a list of services provided by the service provider, the type of services provided, and the geographical location of the service provider. HUAWEI CLOUD has been deployed in multiple regions and AZs around the world, allowing FIs to select data storage locations based on their requirements. If FIs need to submit an annual report to the regulatory authority, HUAWEI CLOUD will arrange a dedicated person to actively cooperate with the financial institution in providing related materials.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
334	Section IV: Final provisions	Institution should consider the following when developing policies relating to third-party service contracts: 1. Capability of a third party to implement measures or plans, including performance, reliability, and business continuity. 2. Completeness, accuracy, security, confidentiality, security, timeliness and reliability, and access control measures in dealing with information relating to services provided or entrusted. 3. Methods used by FIs to assess compliance with contracts. 4. Criteria and procedures for regularly assessing the quality of services. 5. The ability of third parties to provide continuity of contractual services, or alternative options available to the financial institution in any case, to reduce the vulnerability of the institution's operations. 6. Risk tolerance of institutions. 7. The ability of an institution to identify, measure, monitor, limit, control, communicate and disclose risks that may arise from the services described in this chapter in integrated risk management. 8. The ability of the internal control system to comply with this provision.	FIs should establish contracts with third parties in accordance with relevant requirements. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on financial requirements. To provide continuous and stable cloud services for customers, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's audit and supervision rights on HUAWEI CLOUD will be promised in the agreement signed with the customer based on the actual situation. HUAWEI CLOUD has passed multiple

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		9. The Board of Directors shall designate a responsible person, which may be an internal auditor, to monitor, evaluate and report regularly to the Board of Directors on the performance of the service provider and on compliance with applicable provisions. 10. The Board of Directors shall review the third-party supplier selection system at least annually and revise it in the light of the third-party performance evaluation.	international security and privacy protection certifications, including ISO27001, ISO27017, ISO27018, SOC, and CSA STAR, and is audited by a third party every year.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 52	Minimum Security Criteria for Procurement of Technical Support Services	FIs should consider the following security guidelines when purchasing technical support services: 1. Security aspects a. Measures to ensure that sensitive user information is transmitted in point-to-point encryption. b. The financial institution shall establish a security officer independent of the business, audit and system domains. The security officer shall be responsible for managing access control and shall have access to authorized access records. The access records of authorized personnel shall be retained. 2. Audit and oversight a. FIs should audit the security controls and operation of the third party data center infrastructure at least once every two years.	The financial institution shall transmit sensitive information of users in encrypted mode and establish an independent security officer who is authorized to review and audit user information records. The financial institution shall conduct a security audit on the third-party data center at least once every two years to check the implementation of security measures in the third-party data center. In scenarios where data is transmitted between the client and server and between the servers through the public information channel, data protection during transmission is provided in the following ways: Virtual Private Network (VPN): A VPN is used to establish an industry-standard secure and encrypted communication tunnel between a remote network and a VPC, seamlessly extending the existing data center to HUAWEI CLOUD, and providing end-to-end data transmission confidentiality assurance for tenants. VPN establishes communication tunnels between traditional data centers and VPC. Tenants can conveniently use resources such as cloud servers and block storage on HUAWEI CLOUD. Applications can be transferred to the cloud and additional web servers can be started to increase

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			the computing capacity of the network. It also reduces the risk of illegal proliferation of enterprise core data. Currently, HUAWEI CLOUD uses hardware-implemented Internet Key Exchange (IKE) and IPSec VPN to encrypt data transmission channels to ensure transmission security. Application layer TLS and certificate management: HUAWEI CLOUD services provide REST and Highway data transmission. The REST network channel releases services in standard RESTful mode. The caller uses HTTP clients to invoke APIs in standard RESTful mode to implement data transmission. The Highway channel is a high-performance proprietary protocol channel. It can be used when there are special performance requirements. Both data transmission modes support encrypted transmission using Transport Layer Security (TLS) 1.2 and X.509 certificate-based target website identity authentication. SSL Certificate Service (SCM) is a one-stop X.509 certificate lifecycle management service provided by HUAWEI CLOUD and a world-renowned digital certificate service provider to implement trusted identity

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			authentication and secure data transmission for target websites. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by FIs. FIs' rights and interests in auditing and monitoring HUAWEI CLOUD will be promised in agreements signed with FIs based on actual situations.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 64.2	Information Security Incident Report	1. Institutional information a. Name of the institution. b. The full name of the Chief Information Security Officer and his/her telephone number and email address. 2. Attach the following information about information security incidents to encrypted digital media a. Information security incident description. b. Affected accounts. c. Status of the affected account (blocked, suspended, or activated). d. Affected network areas (Internet, intranet, management network, etc.). e. Affected System Type (file servers, network servers, mail services, databases, workstations, mobile devices, etc.). f. Operating system (indicate the version). g. Protocols or services of affected components. h. The number of components of the affected system at the institution. i. Application(s) involved (specified version). j. Information about the damaged device (brand, software	FIs shall promptly report information security incidents to the CNBV Commission in accordance with the information security reports required by the general provisions. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and assist FIs in meeting regulatory notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		version, firmware, etc.). k. Impact of information security incidents on services. l. Amount of loss in pesos. m. Amounts recovered in pesos. n. The status of the information security incident (resolved or unresolved). o. Indicate whether the information security incident has been reported to any authority. If so, please indicate the authorization and date. p. The public IP address, email address, or domain name of the source of the attack. q. Communication Protocols Used. r. Websites involved. s. Detected Malware. t. Describe in detail the actions taken to mitigate the information security incident and refer to those responsible for implementing those mitigation actions. u. Describe the results of mitigation measures. v. In subsequent similar cases, action is taken to minimize losses. w. Other information that you believe should be brought to the	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		attention of the CNBV Commission.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 67	Minimum Requirements for Business Continuity Plans	1. Institutions should conduct a business impact analysis prior to developing a business continuity plan. a. Identify key processes that are integral to business continuity. b. Determine minimum resources (Human, logistical, material, technical infrastructure and resources of any other nature) in order to maintain and rebuild institution services and procedures in the event of an emergency, and at the end of such an emergency. c. Develop relevant scenarios related to the verification of possible operational emergencies, such as: i. Natural and environmental disasters. ii. Communicable diseases. iii. Cyber-attacks or attacks on computer activities. iv. Vandalism. v. Terrorism. vi. Power supply is interrupted. vii. Failure or unavailability of technical infrastructure (telecommunication, information processing and networking).	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on FIs is considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		viii. Inadequate human, material or technical resources. ix. Service provided by a third party is interrupted. d. Assess the quantitative and qualitative impact of the incident based on the scenarios defined for each critical process and through a methodology approved by the Risk Commission. e. Determine recovery priorities for each critical process. f. Determine the Recovery Time Objective (RTO) for each critical process. g. Where appropriate, establish Recovery Point Objective (RPO) as the maximum tolerable data loss for each critical process. h. Identify and assess risks associated with operational processes and data processing and transmission services contracted with suppliers, as well as risks associated with the custody and security of information of the institution or its FIs. i. Determine the risks posed by the geographic location of the primary data center for the critical	continuous running of cloud services based on the requirements of the internal business continuity management system. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. In addition, as a cloud service provider, HUAWEI CLOUD meets organizations' requirements for information security and information security management continuity in the event of a disaster. HUAWEI CLOUD provides customers with the **Storage Disaster Recovery Service (SDRS)** and provides disaster recovery (DR) functions for ECS, EVS disk, and **Dedicated**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		processes identified in accordance with a) of this section to avoid the secondary data center being exposed to the same risks as the primary data center. 2. In developing business continuity plans, institutions should incorporate the following strategies: a. With regard to prevention, consideration should be given to: i. Assess the institution's processes and services to reduce the impact of the vulnerability of the processes and services on business continuity. ii. The availability of the necessary human, financial, material, technical and technological infrastructure resources for timely action in the event of an operational emergency. iii. Establish a program to test the business continuity plan, update it at least annually, and update it in advance if there are significant changes to the institution's technology infrastructure, processes, products and services, or internal organization,	**Distributed Storage Service (DSS)**. The SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high data reliability and service continuity. DRS helps protect service applications. It replicates data and configuration information of ECS to the DR site and allows the server where service applications reside to start and run properly from another location when the server is down, improving service continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and evaluate the business continuity plan. iv. Business Continuity Training Program. v. The communication policy for designing and implementing the business continuity plan shall implement notification of the incident based on the nature of the incident described and the different audiences to which it is communicated. vi. Procedures for registering, following up, tracking and communicating to relevant personnel the results of testing the business continuity plan. b. Emergency events, which shall include the following: i. Identify in a timely manner the nature of the incident affecting the institution's critical processes. ii. Control the impact of incidents on key processes. c. Restoration to bring the institution's services and procedures back to minimum service levels and eventually to normal. d. Assessment, which should include the collection and analysis	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		of relevant information on the development of the incident and the actions and procedures taken to prevent, contain and recover from the incident, with a view to making adjustments to the business continuity plan as necessary.	

6 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Securities Market Law and its General Provisions

The National Banking and Securities Commission (CNBV) has issued the *Securities Market Law and its General Provisions*, which sets out regulations primarily for companies other than fintech institutions involved in securities and equity offerings and intermediaries, as well as the risks that may arise from this activity.

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

6.1 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Securities Market Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
116	Section I: Broker-Dealer Part I: Organization	Brokerage firms shall certify to the CNBV Commission 30 working days prior to the commencement of business: The infrastructure and internal controls necessary for the provision of services by the brokerage firm itself and contracted outsourced service providers may be prohibited from doing business by the CNBV Commission if it is not successfully demonstrated.	Brokerage firms shall provide the CNBV Commission with materials relating to infrastructure and internal controls within 30 working days at the time of application in accordance with this Article. HUAWEI CLOUD will cooperate with FIs to provide related reporting materials.
219	Section II: Business, Activities and Services of Brokers Part VII: Other Provisions	Brokerage firms enter into outsourced service contracts with third parties subject to prior approval from the CNBV Commission and compliance with relevant general provisions.	Brokerage firms shall obtain approval from the CNBV Commission before applying for business in accordance with this Article. HUAWEI CLOUD will cooperate with FIs to provide related reporting materials and implement management requirements for third-party outsourcing services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
220	Section II: Business, Activities and Services of Brokers Part VII: Other Provisions	Brokerage firms entering into outsourced service contracts with third parties shall comply with the following requirements: 1. Submit a report to the CNBV Commission describing the scope of services provided by cloud service providers, risks, and supplier selection criteria and procedures. 2. Develop policies and procedures to monitor cloud service provider performance and contract performance. a. The quality and cost of outsourced services should be considered, and performance objectives and measurement methods should be defined. b. Possibility and limitations of subcontracting. c. Confidentiality and security of information. d. Procedures for testing the performance of the cloud service provider's contractual obligations. e. Require cloud service providers to be audited and supervised and provide records, information and technical support related to the service when required. f. Business continuity plans and emergency response procedures. g. In the case of a foreign cloud service provider, the written consent of the cloud service provider to	FIs should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. HUAWEI CLOUD provides the **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		comply with this Regulation is required. h. Periodically evaluate the performance of cloud service providers and compliance with relevant regulations and submit them to the Board for approval and verification.	
221	Section II: Business, Activities and Services of Brokers Part VII: Other Provisions	1. The brokerage firm's contracting out services with a third party shall not relieve the brokerage firm or its directors and employees of the obligation to comply with the provisions of this Act and the general provisions arising therefrom. 2. The CNBV Commission, through a brokerage firm, may request information from third parties regarding the provision of outsourced services, including books, records and documents.	If FIs sign an outsourcing service with a third party, but cannot outsource legal liabilities, the financial institution or its directors and employees shall bear corresponding responsibilities in accordance with the requirements under this Law. The financial institution shall cooperate with the CNBV Commission to collect relevant information from the financial institution's outsourced service providers. HUAWEI CLOUD will assign dedicated personnel to actively respond to the requirements of financial institution and provide related materials.

6.2 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions Applicable to Stock Exchanges

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
33	Section I: Management and Control of Technology Infrastructure	The Stock Exchange shall develop, document and implement policies and procedures necessary to: 1. Each component of the technology infrastructure is capable of performing the functions stated at the time of its design, development or procurement. 2. Information security issues have been taken into account at all stages of the service lifecycle, including requirement description, design, development, test, and release. 3. The stock exchange shall logically or physically isolate the network into different domains and sub-networks based on different functions or types of data transmitted. 4. The stock exchange shall perform security configuration for the network security components, taking into account factors such as port, least privilege principle, media management, access control, manufacturer update and reconfiguration of factory settings.	FIs shall develop information security management processes and mechanisms for technical infrastructure, including physical security, software lifecycle security management, awareness training, data lifecycle management, access control, vulnerability management, and business continuity management, and ensure that outsourced service providers provide corresponding outsourced services according to the requirements of the general provisions. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		5. The stock exchange shall test the components before deployment or change. During the test, the use of production data or the introduction of unauthorized functions are prohibited. 6. Have a license or authorization to use, if applicable. 7. Establish security protection measures such as access control, communication security, and information security management, including: a. Establish a user identification and authentication mechanism to ensure that only authorized users are allowed access. Access control should include exceptional access authorization policies and procedures in special cases. b. For technical infrastructure users with high privileges, such as database and operating system administrators, a privileged account management system shall be established. c. Have password management measures to prevent access by unauthorized users. d. The stock exchange shall classify its information by level	management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, Public Service, Point of Delivery (POD), Object-Based Storage (OBS), and Operations Management (OM). In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and encrypt sensitive information. e. The stock exchange shall establish a session management mechanism to automatically close unattended sessions and prevent unauthorized simultaneous use of sessions of the same user identity. f. The stock exchange shall establish physical access control. 8. The technical infrastructure has backup mechanisms and recovery procedures. 9. Maintain a complete audit log, including accesses or attempts to access information, as well as records of operations or activities performed by users of the technology infrastructure. 10. The stock exchange should establish an information security incident management process and designate a team to manage and implement it. 11. Conduct annual planning and review of the technology infrastructure and develop an update plan. 12. The technical infrastructure should implement automatic control measures or, in the absence of automatic control measures, compensatory controls to	smallest attack surface and is relatively easy to control security risks. For details about security zones, see **HUAWEI CLOUD Security White Paper.** HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. FIs can use the **Identity and Access Management (IAM)** of HUAWEI CLOUD to manage user accounts that use cloud resources. Administrators can plan users' permissions

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		reduce the risk of manual or semi-automatic control procedures. 13. Establish controls to prevent tampering or falsification of assets, books and records. 14. Establish procedures to measure the level of availability of internal and external services and service response times. 15. Conduct vulnerability and threat detection at least annually or as any part of its technology infrastructure changes, as well as penetration testing of different parts of its technology infrastructure.	to use cloud resources based on their work responsibilities and set security policies for users to access cloud service systems, such as access control list (ACL), to prevent malicious access from untrusted networks. **Cloud Trace Service (CTS)** of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. **Cloud Eye Service (CES)** of HUAWEI CLOUD provides a three-dimensional monitoring platform for Elastic Cloud Server (ECS) and bandwidth resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately understand service resource status. Users can set alarm rules and notification policies to learn about the running status and performance of each service instance. FIs can use **Vulnerability Scan Service (VSS)**of HUAWEI CLOUD to implement functions such as web

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			vulnerability scanning, OS vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks that websites or servers are exposed to on the network to implements multi-dimensional security detection for services on the cloud. Financial institution can use the **Data Encryption Workshop (DEW)** of HUAWEI CLOUD to encrypt data. Currently, multiple services of HUAWEI CLOUD, such as **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, and **Image Management Service (IMS)**, provide data encryption (server-side encryption) for FIs. In addition, FIs can centrally manage keys throughout their lifecycle through data encryption services. The hardware security module (HSM) used by HUAWEI CLOUD creates and manages keys for FIs. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, meeting users' data compliance requirements and preventing intrusion and tampering. Even

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI O&M personnel cannot steal the root key of FIs. DEW also allows financial institution to import their own keys as their master keys for unified management, facilitating seamless integration and interconnection with existing services of financial institution. In addition, HUAWEI CLOUD uses customer master key online redundancy storage and multiple physical offline backups of root keys to ensure key persistence. For more information, see HUAWEI CLOUD Security White Paper. When financial institution provides web services over the Internet, it can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. By applying for and configuring a certificate for a Web site, the trusted identity authentication and protocol-based secure transmission of the Web site can be implemented. In hybrid cloud deployment and global deployment scenarios of FIs, services such as **Virtual Private Network (VPN)**,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Direct Connect (DC), and **Cloud Connect (CC)** provided by HUAWEI CLOUD can be used to implement service interconnection and data transmission security between different regions. **Host Security Service (HSS)** of HUAWEI CLOUD is a security manager for servers. It provides asset management functions for FIs, including managing and analyzing security asset information such as accounts, ports, processes, web directories, and software. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement DR and backup of their service systems. HUAWEI CLOUD also provides training services for FIs, including help documents, user manuals, and security implementation guides. For more training services and resources provided by HUAWEI CLOUD for FIs, see "Training Services" on the official website. To meet customers' compliance requirements, HUAWEI CLOUD regularly conducts internal and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
37	Section II: Business Continuity Plan	The general manager of the Stock Exchange shall establish a Business Continuity Plan, which and its modifications shall be submitted to the Board of Directors for approval through the Audit Committee. The general manager shall be responsible for: 1. Develop a training plan, implement, continuously update and disseminate the plan. 2. Design and implement a communication policy for the Business Continuity Plan and communicate in a timely manner with FIs, the public, the CNBV Commission and other competent authorities according to the nature of the emergency in question. 3. When an emergency occurs, update the CNBV Commission on the situation and submit an analysis report to the CNBV Commission within 15 calendar days after the end of the emergency, describing the causes and effects of the emergency. 4. Conduct a validity test on the business continuity plan at least once a year and ensure that the business continuity plan is reviewed or updated annually.	FIs should identify their key business processes and develop business continuity plans. The financial institution shall test the effectiveness of the business continuity plan at least annually, communicate the results of the test to the Board of Directors and the CNBV Commission, and update the plan on an ongoing basis based on the results of the test and the recommendations of the CNBV Commission. The financial institution shall develop a method for assessing the impact of an emergency. When an emergency occurs, the financial institution shall notify the CNBV Commission and explain the cause and impact of the emergency. HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the IS022301 certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
38	Section II: Business Continuity Plan	The stock exchange shall develop a methodology for assessing the quantitative and qualitative impact of an incident, with the prior approval of the Board of Directors. The Audit Committee shall annually verify the effectiveness of the methodology, make amendments based on the reported results, and report the results of this test and evaluation to the Board of Directors and the CNBV Commission.	emergency response mechanism. If FIs need HUAWEI CLOUD to participate in the development and execution of its business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 6	Minimum Requirements for Business Continuity Plans	1. Institutions should conduct a business impact analysis prior to developing a business continuity plan. a. Identify key processes that are integral to business continuity. b. Determine minimum resources (Human, logistical, material, technical infrastructure and resources of any other nature) in order to maintain and re-establish stock exchange services and procedures in the event of an operational emergency and at the end of such an emergency. c. Prepare a plan relating to possible emergencies, taking into account, among other things, the following: i. Natural and environmental disasters. ii. Communicable diseases. iii. Cyber-attacks or attacks on computer activities. iv. Vandalism. v. Terrorism. vi. Power supply is interrupted. vii. Failure or unavailability of technical infrastructure (telecommunication, information processing and networking).	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		viii. Inadequate human, material or technical resources. ix. Service provided by a third party is interrupted. d. Assess the quantitative and qualitative impact of the incident based on the scenarios defined for each critical process. e. Define recovery priorities for each critical process. f. Determine Recovery Time Objective (RTO) for each service and process. g. Consider the Recovery Point Objective (RPO), which is understood as the maximum data loss that can be tolerated by each service and process, considering that under no circumstances can the transaction information that has been entered be lost, and keeping abreast of the status of each transaction in the event of an emergency. h. Identify and assess risks associated with operational processes and data processing and transmission services contracted with service providers, as well as risks associated with the custody and security of information on stock	FIs is considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		exchanges or brokerage firms. i. Determine the risks posed by the geographic location of the primary data center for the critical processes identified in accordance with a) of this section to avoid the secondary data center being exposed to the same risks as the primary data center. j. Consider establishing standby data processing and operations sites, which should be able to operate on a required basis and should not be subject to the same risks as the primary site. 2. In developing business continuity plans, institutions should incorporate the following strategies: a. In terms of prevention, the following should be taken into account: i. Assess the institution's processes and services to reduce the impact of the vulnerability of the processes and services on business continuity. ii. The availability of the necessary human, financial, material, technical and technological infrastructure resources for timely	In addition, as a cloud service provider, HUAWEI CLOUD meets organizations' requirements for information security and information security management continuity in the event of a disaster. HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS) and provides disaster recovery (DR) functions for ECS, EVS disk, and Dedicated Distributed Storage Service (DSS). The SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high data reliability and service continuity. DRS helps protect service applications. It replicates data and configuration information of ECS to the DR site and allows the server where service applications reside to start and run properly from another location when the server is down, improving service continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		action in the event of an operational emergency. iii. Establish a program to test the business continuity plan, update it at least annually, and update it in advance if there are significant changes to the institution's technology infrastructure, processes, products and services, or internal organization, and evaluate the business continuity plan. iv. Business Continuity Training Program. v. The communication policy for designing and implementing the business continuity plan shall implement notification of the incident based on the nature of the incident described and the different audiences to which it is communicated. vi. Procedures for registering, following up, tracking and communicating to relevant personnel the results of testing the business continuity plan. b. Emergency events, which shall include the following: i. Identify in a timely manner the nature of the incident affecting	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the institution's critical processes. ii. Control the impact of incidents on key processes. c. Restoration to bring the institution's services and procedures back to minimum service levels and eventually to normal. d. Assessment, which should include the collection and analysis of relevant information on the development of the incident and the actions and procedures taken to prevent, contain and recover from the incident, with a view to making adjustments to the business continuity plan as necessary.	

6.3 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions Applicable to Brokerage Companies

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
117.2.7	Section I: Internal Controls Part VI: Overall Management	Brokerage firms shall develop, document and implement policies and procedures necessary to: 1. Each component of the technology infrastructure is capable of performing the functions stated at the time of its design, development or procurement. 2. Ensure the integrity and adequate maintenance of the technical infrastructure. 3. Information security issues are taken into account at all stages of the service lifecycle, including requirement description, design, development, test, and release. 4. FIs should logically or physically isolate networks into different domains and sub-networks based on different functions or types of data transmitted. 5. FIs should configure security for network security	FIs shall develop information security management processes and mechanisms for technical infrastructure, including physical security, software lifecycle security management, awareness training, data lifecycle management, access control, vulnerability management, and business continuity management, and ensure that outsourced service providers provide corresponding outsourced services according to the requirements of the general provisions. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		components, taking into account factors such as ports, least privilege principles, media management, access control, manufacturer updates and reconfigurations of factory settings. 6. FIs should test components before deployment or change. Do not use production data or introduce unauthorized functions during the tests. 7. Have a license or authorization to use, if applicable. 8. Establish security protection measures such as access control, communication security, and information security management, including: a. Establish a user identification and authentication mechanism to ensure that only authorized users are allowed access. Access control should include exceptional access authorization policies and procedures in special cases.	systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, Public Service, Point of Delivery (POD), Object-Based Storage (OBS), and Operations Management (OM). In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		b. For technical infrastructure users with high privileges, such as database and operating system administrators, a privileged account management system shall be established. c. Have password management measures to prevent access by unauthorized users. d. FIs should classify their information in a hierarchical manner and encrypt sensitive information. e. FIs shall establish session management mechanisms to automatically close unattended sessions and prevent unauthorized simultaneous use of sessions of the same user identity, f. FIs should establish physical access controls. 9. The technical infrastructure has backup mechanisms and recovery procedures. 10. Maintain a complete audit log,	relatively easy to control security risks. For details about security zones, see HUAWEI CLOUD Security White Paper. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. FIs can use the IAM of HUAWEI CLOUD to manage user accounts that use cloud resources. Administrators can plan users' permissions to use cloud resources based on their work responsibilities and set security policies for users to access cloud service systems, such as access control list (ACL), to prevent malicious access from untrusted networks. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		including accesses or attempts to access information, as well as records of operations or activities performed by users of the technology infrastructure. 11. FIs should establish information security incident management procedures and designate a team to manage and implement them. 12. Conduct annual planning and review of the technology infrastructure and develop an update plan. 13. The technical infrastructure should implement automatic control measures or, in the absence of automatic control measures, compensatory controls to reduce the risk of manual or semi-automatic control procedures. 14. Establish controls for the tampering or falsification of assets, books, records and digital documents. 15. Establish procedures to measure the level of availability of internal and external services	scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. Cloud Eye Service (CES) of HUAWEI CLOUD provides a three-dimensional monitoring platform for Elastic Cloud Server (ECS) and bandwidth resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately understand service resource status. Users can set alarm rules and notification policies to learn about the running status and performance of each service instance. FIs can use Vulnerability Scan Service (VSS) of HUAWEI CLOUD to implement functions such as web vulnerability scanning, OS vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks that websites or servers are exposed to on the network to implements multi-dimensional security detection for services on the cloud. Financial institution can use the Data Encryption Workshop (DEW) of HUAWEI CLOUD to encrypt data. Currently, multiple services of HUAWEI CLOUD, such as Elastic Volume Service (EVS), Object Storage Service (OBS), and Image Management Service (IMS), provide data encryption (server-side encryption) for

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		and service response times. 16. Conduct vulnerability and threat detection at least annually or when any part of its technology infrastructure changes, as well as penetration testing of different parts of its technology infrastructure.	FIs. In addition, FIs can centrally manage keys throughout their lifecycle through data encryption services. The hardware security module (HSM) used by HUAWEI CLOUD creates and manages keys for FIs. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, meeting users' data compliance requirements and preventing intrusion and tampering. Even HUAWEI O&M personnel cannot steal the root key of FIs. DEW also allows financial institution to import their own keys as their master keys for unified management, facilitating seamless integration and interconnection with existing services of financial institution. In addition, HUAWEI CLOUD uses customer master key online redundancy storage and multiple physical offline backups of root keys to ensure key persistence. For more information, see HUAWEI CLOUD Security White Paper. When financial institution provides web services over the Internet, it can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. By applying for and configuring a certificate for a Web site, the trusted identity authentication and protocol-based secure transmission of the Web site can be implemented. In hybrid

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			cloud deployment and global deployment scenarios of FIs, services such as Virtual Private Network (VPN), Direct Connect (DC), and Cloud Connect (CC) provided by HUAWEI CLOUD can be used to implement service interconnection and data transmission security between different regions. Host Security Service (HSS) of HUAWEI CLOUD is a security manager for servers. It provides asset management functions for FIs, including managing and analyzing security asset information such as accounts, ports, processes, web directories, and software. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement DR and backup of their service systems. HUAWEI CLOUD also provides training services for FIs, including help documents, user manuals, and security implementation guides. For more training services and resources provided by HUAWEI CLOUD for FIs, see "Training Services" on the official website. To meet customers' compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			security threats to ensure the security of cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206	Section II: Outsourcing Services to Third Parties	Brokerage firms should comply with the following requirements when entering into service contracts with third parties. 1. Provide a report on the criteria and policies for selecting third-party service providers. 2. Specify in the service contract or in a document unconditionally accepted by a third party: a. Accept visits to the physical premises by the Broker's external auditors and the CNBV Commission, and the Broker may appoint a representative to accompany the visit. b. Audit of the services covered by the contract by the brokerage firm or through a third party designated by the CNBV Commission itself. c. Provide books, systems, records, manuals relating to the provision of services to the external auditors of brokerage firms and to	FIs should establish contracts with third parties in accordance with relevant requirements. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD receives audits from professional third-party audit organizations every year and provides dedicated personnel to actively respond to and cooperate with audit activities initiated by customers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		third parties designated by the CNBV Commission or CNBV Commission at the request of the brokerage firm, and shall also allow responsible persons access to offices and facilities relating to the services rendered. 3. Policies and procedures exist to monitor third parties' performance and performance of their contractual obligations. Such policies and procedures should include matters relating to: a. The brokerage firm's ownership of the data generated by the service. b. Ensure that service providers receive adequate training on a regular basis in relation to contracted services. c. If the contracted services involve the use of technology or telecommunicati ons	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		infrastructure, the minimum security guidelines set out in Annex 12 to this Regulation shall be observed. 4. Audits are conducted every two years to verify compliance with this chapter and minimum security guidelines, if applicable, and the results are reported to the Board of Directors and the Audit Committee. 5. To require the general manager, the Audit Committee and the internal auditors of the brokerage firm to oversee, in accordance with their authority, the technology used by the outsourced service provider to provide services, the information processing infrastructure and the information processing, control and security mechanisms.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2	Section II: Outsourcing Services to Third Parties	1. Brokerage firms should establish standards and contract with outsourced service providers should consider: a. The institution has the ability to maintain business continuity in the event of an emergency. b. The complexity and time required to find a third party to replace the original contracting party. c. Restrictions in making decisions that have a significant impact on the administrative, financial, operational or legal situation of the institution itself. d. The institution's ability to maintain adequate internal controls and to comply with regulatory requirements in the event of a third party suspension of services. e. The impact that the suspension of services will have	The general manager of FIs is the main person responsible for the outsourcing management of FIs. The financial institution shall, in accordance with the general provisions, formulate the outsourcing management mechanism and determine the criteria for signing contracts with the outsourcing service provider and submit the relevant information to the CNBV Commission for approval 20 working days prior to signing the contract with the outsourced service provider. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		on the institution's financial, reputation and operations. f. Vulnerability of financial institution information. 2. The general manager of the financial institution shall be responsible for approving the selection policies and criteria for third-party service providers. 3. The brokerage firm shall submit to the Regulatory CNBV Commission, and obtain consent, 20 working days prior to the conclusion of the contract with the outsourced service provider, a notice of the operational, technical or database management process for the service object concerned.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2.1	Section II: Outsourcing Services to Third Parties	The notice referred to in No. 206.2 shall be signed by the general head of the financial institution and, if the service involves the use of technology or telecommunications infrastructure, the notice shall contain an additional technical report specifying the type of banking business or service carried out using the technology infrastructure provided by third parties and compliance with the minimum security guidelines for the procurement of services under this provision.	FIs are required to submit relevant materials to the CNBV Commission and obtain approval before they plan to enter into service contracts with third parties. To meet customers' compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. If the customer applies for this document, HUAWEI CLOUD will provide the customer with copies of related documents as required. HUAWEI CLOUD will cooperate with FIs to provide related reporting materials

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and implement supervision notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2.2	Section II: Outsourcing Services to Third Parties	Brokerage firms shall request the CNBV Commission's authorization to enter into contracts with third parties for outsourced services, and if the services are partly or wholly provided or performed outside the national territory or by residents abroad, the brokerage firms shall apply for such authorization to the Vice-President of the CNBV Commission responsible for supervision at least 20 working days prior to the conclusion of the contract and submit the following documents. 1. Information about the country in which the third party or entrusted agent with whom the contract is concluded resides, the protection measures provided by its domestic law for personal data, or the country of residence has entered into an international agreement with Mexico on such matters. 2. Institutions must declare to the CNBV Commission that they will maintain at least the	FIs should establish contracts with third parties in accordance with relevant requirements. When FIs enter into an outsourced service contract with an institution outside Mexico or with a resident outside Mexico, it shall apply to and obtain authorization from the CNBV Commission 20 working days prior to the conclusion of the contract. When applying to the CNBV Commission, FIs shall provide the relevant documents as required by these general provisions. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD will cooperate with the customer to provide related reporting materials and to cooperate with the customer to implement the supervision notice.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		documents and information relating to evaluations, audit findings and performance reports at their principal offices located in the United Mexican States. Similarly, when requested by the CNBV Commission, they shall provide Spanish-language versions of such documents. 3. The brokerage firm has been approved by the Board of Directors, or by the Audit Committee or Risk Committee, and has stated in their respective agreements that entering into a service or commission contract will not jeopardize full compliance with the provisions applicable to the institution.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2.4	Section II: Outsourcing Services to Third Parties	When the CNBV Commission believes that an institution's financial stability, business continuity, or protection of the public interest may be affected, or the institution fails to comply with this and other applicable provisions, the CNBV Commission may, after the institution has been granted the right to a hearing, Order the partial or total, temporary or final suspension of services or commissions provided through the third party concerned. Unless, in the exercise of the hearing right, the financial institution submits a formalization plan for review by the CNBV Commission, which makes an appropriate decision within 30 calendar days.	When the CNBV Commission considers that the financial institution does not meet the requirements of this general provisions, the financial institution shall cooperate in submitting a standardized proposal for review by the CNBV Commission and may suspend the contract with the relevant third party if necessary. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and fulfill regulatory requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2.5	Section II: Outsourcing Services to Third Parties	Brokerage firms should have a list of service providers which should include, at a minimum, the following information. FIs should have a list of service providers which should include, at a minimum, the following information. 1. Name of the service provider and company. 2. Name of the legal representative of the service provider. 3. Describe the services contracted with the third party, including the data or information stored or processed by the third party, if any. 4. If applicable, system information relating to services provided by third parties, including at least the system name, version and function or purpose. 5. Interfaces with other systems and their purpose, including details of the exchange of information. 6. The full address at which the service is performed and the location of the person responsible for performing the service.	FIs shall develop and maintain a list of its suppliers, which shall include the basic information of the service provider, including the name of the service provider, details of the services provided, etc. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and fulfill regulatory requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		7. If applicable, the full address of the primary data center in which the processing equipment of the Contract System is located. 8. Where applicable, the full address of the standby data center in which the processing equipment is located. 9. The date of the broker-dealer's notification to the CNBV Commission. 10. The number and date of the notice to obtain approval to contract services.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
206.2.6	Section II: Outsourcing Services to Third Parties	Brokerage firms should consider the following when developing policies relating to service or commission contracts: 1. Capability of a third party to implement measures or plans, including performance, reliability, capability, and business continuity. 2. Completeness, accuracy, security, confidentiality, security, timeliness and reliability of information generated in connection with the provision of services or commissions, as well as access control measures. 3. Methods that brokerage firms can use to assess compliance with contracts. 4. Criteria and procedures for regularly assessing the quality of services. 5. The ability of third parties to provide continuity of contractual services, or alternative options available to the brokerage in any event, to reduce the fragility of the brokerage's operations.	The Customer shall establish contracts with third parties in accordance with the relevant requirements. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer. The customer's audit and supervision rights on HUAWEI CLOUD will be promised in the agreement signed with the customer based on the actual situation. HUAWEI CLOUD has passed multiple international security and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		6. Risk tolerance of economic firms. 7. Brokerage firms identify, measure, monitor, limit, control, communicate and disclose risks that may arise from the services described in this chapter in integrated risk management. 8. The ability of the internal control system to comply with this provision. 9. The Board of Directors shall designate a responsible person, which may be an internal auditor or an audit committee, to monitor, evaluate and regularly report to the Board on the performance of the service provider and compliance with applicable rules relating to the corresponding service or transaction. 10. The system for selecting third parties shall be reviewed by the Board of Directors at least annually and modified in the light of the results of the third party performance evaluation.	privacy protection certifications, including ISO27001, ISO27017, ISO27018, SOC, and CSA STAR, and is audited by a third party every year.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 12	Financial institutions should consider the following safety guidelines when purchasing	FIs should consider the following security guidelines when purchasing technical support services: 1. Security aspects a. Measures to ensure that sensitive user information is transmitted in point-to-point encryption. b. The financial institution shall establish a security officer independent of the business, audit and system domains. The security officer shall be responsible for managing access control and shall have access to authorized access records. The access records of authorized personnel shall be retained. 2. Audit and oversight a. FIs should audit the security controls and operation of the third party data center infrastructure at least once every two years.	The financial institution shall transmit sensitive information of users in encrypted mode and establish an independent security officer who is authorized to review and audit user information records. The financial institution shall conduct a security audit on the third-party data center at least once every two years to check the implementation of security measures in the third-party data center. In scenarios where data is transmitted between the client and server and between the servers through the public information channel, data protection during transmission is provided in the following ways: **Virtual Private Network (VPN):** A VPN is used to establish an industry-standard secure and encrypted communication tunnel between a remote network and a VPC, seamlessly extending the existing data center to HUAWEI CLOUD, and providing end-to-end data transmission confidentiality assurance for tenants. VPN establishes communication tunnels between traditional data centers and VPC. Tenants can conveniently use resources such as cloud servers and block storage on HUAWEI CLOUD. Applications can be transferred to the cloud and additional web servers can be started to increase the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			computing capacity of the network. It also reduces the risk of illegal proliferation of enterprise core data. Currently, HUAWEI CLOUD uses hardware-implemented Internet Key Exchange (IKE) and IPSec VPN to encrypt data transmission channels to ensure transmission security. **Application layer TLS and certificate management:** HUAWEI CLOUD services provide REST and Highway data transmission. The REST network channel releases services in standard RESTful mode. The caller uses HTTP clients to invoke APIs in standard RESTful mode to implement data transmission. The Highway channel is a high-performance proprietary protocol channel. It can be used when there are special performance requirements. Both data transmission modes support encrypted transmission using Transport Layer Security (TLS) 1.2 and X.509 certificate-based target website identity authentication. SSL Certificate Service (SCM) is a one-stop X.509 certificate lifecycle management service provided by HUAWEI CLOUD and a world-renowned digital certificate service provider to implement trusted identity authentication and secure data transmission for target websites.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by FIs. FIs' rights and interests in auditing and monitoring HUAWEI CLOUD will be promised in agreements signed with FIs based on actual situations.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 18	Minimum Requirements for Business Continuity Plans	1. Institutions should conduct a business impact analysis prior to developing a business continuity plan. a. Identify key processes that are integral to business continuity. b. Determine minimum resources (Human, logistical, material, technical infrastructure and resources of any other nature) in order to maintain and rebuild the services and procedures of the brokerage firm in the event of an emergency and at the end of such an emergency. c. Prepare a plan related to possible incidents, taking into account at least the following points: i. Natural and environmental disasters. ii. Communicable diseases. iii. Cyber-attacks or attacks on	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on FIs is considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support continuous running of cloud services based on the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		computer activities. iv. Vandalism. v. Terrorism. vi. Power supply is interrupted. vii. Failure or unavailability of technical infrastructure (telecommunication, information processing and networking). viii. Inadequate human, material or technical resources. ix. Service provided by a third party is interrupted. d. Assess the quantitative and qualitative impact of the incident based on the scenarios defined for each critical process. e. Prioritize recovery for each critical process. f. Determine Recovery Time Objective (RTO) for each service and process. g. Consider the Recovery Point Objective (RPO), which is understood as the maximum tolerable data	requirements of the internal business continuity management system. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. In addition, as a cloud service provider, HUAWEI CLOUD meets organizations' requirements for information security and information security management continuity in the event of a disaster. HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS) and provides disaster recovery (DR) functions for ECS, EVS disk, and Dedicated Distributed Storage Service (DSS). The SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high data

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		loss for each service and process. h. Identify and assess risks associated with the operating processes and data processing and transmission services contracted with the Supplier, as well as risks associated with the custody and security of the information of the Broker or its financial institution. i. Determine the risks posed by the geographic location of the primary data center for the critical processes identified in accordance with a) of this section to avoid the secondary data center being exposed to the same risks as the primary data center. j. Consider establishing standby data processing and operations sites, which should be able to operate on a required basis and should not be subject to	reliability and service continuity. DRS helps protect service applications. It replicates data and configuration information of ECS to the DR site and allows the server where service applications reside to start and run properly from another location when the server is down, improving service continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the same risks as the primary site. 2. In developing business continuity plans, institutions should incorporate the following strategies: a. With regard to prevention, consideration should be given to: i. Assess the institution's processes and services to reduce the impact of the vulnerability of the processes and services on business continuity. ii. The availability of the necessary human, financial, material, technical and technological infrastructure resources for timely action in the event of an operational emergency. iii. Establish a program to test the business continuity plan, update it at least annually, and update it in advance if there are significant changes to the institution's	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		technology infrastructure, processes, products and services, or internal organization, and evaluate the business continuity plan. iv. Business Continuity Training Program. v. The communication policy for designing and implementing the business continuity plan shall implement notification of the incident based on the nature of the incident described and the different audiences to which it is communicated. vi. Procedures for registering, following up, tracking and communicating to relevant personnel the results of testing the business continuity plan. b. Emergency events, which shall include the following: i. Identify in a timely manner	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the nature of the incident affecting the institution's critical processes. ii. Control the impact of incidents on key processes. c. Restoration to bring the institution's services and procedures back to minimum service levels and eventually to normal. d. Assessment, which should include the collection and analysis of relevant information on the development of the incident and the actions and procedures taken to prevent, contain and recover from the incident, with a view to making adjustments to the business continuity plan as necessary.	

6.4 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions Applicable to Securities Depository Institutions

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
23	Section I: Management and Control of Technological Infrastructure	FIs should establish policies and procedures necessary to develop, document and implement: 1. Each component of the technology infrastructure is capable of performing the functions stated at the time of its design, development or procurement. 2. Information security issues are taken into account at all stages of the service lifecycle, including requirement description, design, development, test, and release. 3. FIs should logically or physically isolate networks into different domains and sub-networks based on different functions or types of data transmitted. 4. FIs should configure security for network security components,	FIs shall develop information security management processes and mechanisms for technical infrastructure, including physical security, software lifecycle security management, awareness training, data lifecycle management, access control, vulnerability management, and business continuity management, and ensure that outsourced service providers provide corresponding outsourced services according to the requirements of the general provisions. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive systems, processes, and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		taking into account factors such as ports, least privilege principles, media management, access control, manufacturer updates and reconfigurations of factory settings. 5. FIs should test components before deployment or change. Do not use production data or introduce unauthorized functions during the tests. 6. Have a license or authorization to use, if applicable. 7. Establish security protection measures such as access control, communication security, and information security management, including: a. Establish a user identification and authentication mechanism to ensure that only authorized users are allowed access. Access control should include exceptional access	automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, Public Service, Point of Delivery (POD), Object-Based Storage (OBS), and Operations Management (OM). In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. For details about security zones, see

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		authorization policies and procedures in special cases. b. For technical infrastructure users with high privileges, such as database and operating system administrators, a privileged account management system shall be established. c. Have password management measures to prevent access by unauthorized users. d. FIs should classify their information in a hierarchical manner and encrypt sensitive information. e. FIs shall establish session management mechanisms to automatically close unattended sessions and prevent unauthorized simultaneous use of sessions of the same user identity,	HUAWEI CLOUD Security White Paper. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. FIs can use the IAM of HUAWEI CLOUD to manage user accounts that use cloud resources. Administrators can plan users' permissions to use cloud resources based on their work responsibilities and set security policies for users to access cloud service systems, such as access control list (ACL), to prevent malicious access from untrusted networks. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		f. FIs should establish physical access controls. 8. The technical infrastructure has backup mechanisms and recovery procedures. 9. Maintain a complete audit log, including accesses or attempts to access information, as well as records of operations or activities performed by users of the technology infrastructure. 10. FIs should establish information security incident management procedures and designate a team to manage and implement them. 11. Conduct annual planning and review of the technology infrastructure and develop an update plan. 12. The technical infrastructure should implement automatic control measures or, in the absence of automatic control measures, compensatory	locating. Cloud Eye Service (CES) of HUAWEI CLOUD provides a three-dimensional monitoring platform for Elastic Cloud Server (ECS) and bandwidth resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately understand service resource status. Users can set alarm rules and notification policies to learn about the running status and performance of each service instance. FIs can use Vulnerability Scan Service (VSS) of HUAWEI CLOUD to implement functions such as web vulnerability scanning, OS vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks that websites or servers are exposed to on the network to implements multi-dimensional security detection for services on the cloud. Financial institution can use the Data Encryption Workshop (DEW) of HUAWEI CLOUD to encrypt data. Currently, multiple services of HUAWEI CLOUD, such as Elastic Volume Service (EVS), Object Storage Service (OBS), and Image Management Service (IMS), provide data encryption (server-side encryption) for FIs. In addition, FIs can centrally manage keys throughout their lifecycle through data encryption services. The

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		controls to reduce the risk of manual or semi-automatic control procedures. 13. Establish controls for the tampering or falsification of assets, books, records and digital documents. 14. Establish procedures to measure the level of availability of internal and external services and service response times. 15. Conduct vulnerability and threat detection at least annually or when any part of its technology infrastructure changes, as well as penetration testing of different parts of its technology infrastructure.	hardware security module (HSM) used by HUAWEI CLOUD creates and manages keys for FIs. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, meeting users' data compliance requirements and preventing intrusion and tampering. Even HUAWEI O&M personnel cannot steal the root key of FIs. DEW also allows financial institution to import their own keys as their master keys for unified management, facilitating seamless integration and interconnection with existing services of financial institution. In addition, HUAWEI CLOUD uses customer master key online redundancy storage and multiple physical offline backups of root keys to ensure key persistence. For more information, see HUAWEI CLOUD Security White Paper. When financial institution provides web services over the Internet, it can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. By applying for and configuring a certificate for a Web site, the trusted identity authentication and protocol-based secure transmission of the Web site can be implemented. In hybrid cloud deployment and global deployment scenarios of FIs, services such as Virtual Private Network (VPN), Direct Connect (DC), and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Cloud Connect (CC) provided by HUAWEI CLOUD can be used to implement service interconnection and data transmission security between different regions. Host Security Service (HSS) of HUAWEI CLOUD is a security manager for servers. It provides asset management functions for FIs, including managing and analyzing security asset information such as accounts, ports, processes, web directories, and software. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement DR and backup of their service systems. HUAWEI CLOUD also provides training services for FIs, including help documents, user manuals, and security implementation guides. For more training services and resources provided by HUAWEI CLOUD for FIs, see "Training Services" on the official website. To meet customers' compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
27	Section II: Business Continuity Plan	The general manager of the Stock Exchange shall establish a Business Continuity Plan, which and its modifications shall be submitted to the Board of Directors for approval through the Audit Committee. The general manager shall be responsible for: 1. Develop a training plan, implement, continuously update and disseminate the plan. 2. Design and implement a communication policy for the business continuity plan, including timely communication with FIs and the public, with adversaries, with different administrative and operational units of the institution itself, and with the CNBV Commission and other competent authorities depending on the nature of the emergency in question. 3. In the event of an emergency, update the CNBV Commission on	FIs should identify their key business processes and develop business continuity plans. The financial institution shall test the effectiveness of the business continuity plan at least annually, communicate the results of the test to the Board of Directors and the CNBV Commission, and update the plan on an ongoing basis based on the results of the test and the recommendations of the CNBV Commission. The financial institution shall develop a method for assessing the impact of an emergency. When an emergency occurs, the financial institution shall notify the CNBV Commission and explain the cause and impact of the emergency. HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the IS022301 certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If FIs need HUAWEI CLOUD to participate in the development and execution of its business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the situation and submit an analysis report to the CNBV Commission within 15 calendar days after the emergency, describing the causes and effects of the emergency. 4. Conduct an effectiveness test on business continuity at least once a year and ensure that the business continuity plan is reviewed or updated annually.	
28	Section II: Business Continuity Plan	FIs should develop methods for assessing the quantitative and qualitative impact of emergencies, which should be approved in advance by the CNBV Commission and the Banxico. The Audit Committee shall annually verify the effectiveness of the methodology, make amendments based on the reported results, and report the results of this test and evaluation to the CNBV Commission and the Banxico.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 1	Minimum Requirements for Business Continuity Plans	1. Institutions should conduct a business impact analysis prior to developing a business continuity plan. a. Identify key processes that are integral to business continuity. b. Determine minimum resources (Human, logistical, material, technical infrastructure and resources of any other nature) in order to maintain and rebuild the services and procedures of the Securities Depository upon the occurrence of an emergency and upon its termination. c. Describe the relevant scenarios related to possible operational contingencies, considering at least the following: i. Natural and environmental disasters.	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on FIs is considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		ii. Communicable diseases. iii. Cyber-attacks or attacks on computer activities. iv. Vandalism. v. Terrorism. vi. Power supply is interrupted. vii. Failure or unavailability of technical infrastructure (telecommunication, information processing and networking). viii. Inadequate human, material or technical resources. ix. Service provided by a third party is interrupted. d. Assess the quantitative and qualitative impact of the incident based on the scenarios defined for each critical process. e. Define recovery priorities for each critical process.	business continuity management system. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. In addition, as a cloud service provider, HUAWEI CLOUD meets organizations' requirements for information security and information security management continuity in the event of a disaster. HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS) and provides disaster recovery (DR) functions for ECS, EVS disk, and Dedicated Distributed Storage Service (DSS). The SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high data reliability and service

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		f. Determine Recovery Time Objectives (RTO) for each service and process. g. Consider understanding the Recovery Point Objective (RPO) as the maximum data loss that can be tolerated by each service and process. h. Identify and assess risks associated with operational processes and data processing and transmission services contracted with suppliers, as well as risks associated with the custody and security of securities deposited by the institution or information of its FIs. i. Determine the risks posed by the geographic location of the primary data center for the critical processes identified in accordance with a) of this section to avoid	continuity. DRS helps protect service applications. It replicates data and configuration information of ECS to the DR site and allows the server where service applications reside to start and run properly from another location when the server is down, improving service continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the secondary data center being exposed to the same risks as the primary data center. j. Consider establishing standby data processing and operations sites, which should be able to operate on a required basis and should not be subject to the same risks as the primary site. 2. In developing business continuity plans, institutions should incorporate the following strategies: a. With regard to prevention, consideration should be given to: i. Assess the institution's processes and services to reduce the impact of the vulnerability of the processes and services on business continuity. ii. The availability of the necessary	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		human, financial, material, technical and technological infrastructure resources for timely action in the event of an operational emergency. iii. Establish a program to test the business continuity plan, update it at least annually, and update it in advance if there are significant changes to the institution's technology infrastructure, processes, products and services, or internal organization, and evaluate the business continuity plan. iv. Business Continuity Training Program. v. The communication policy for designing and implementing the business continuity plan shall implement notification of the incident	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		based on the nature of the incident described and the different audiences to which it is communicated. vi. Procedures for registering, following up, tracking and communicating to relevant personnel the results of testing the business continuity plan. b. Emergency events, which shall include the following: i. Identify in a timely manner the nature of the incident affecting the institution's critical processes. ii. Control the impact of incidents on key processes. c. Restoration to bring the institution's services and procedures back to minimum service levels and eventually to normal. d. Assessment, which should	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		include the collection and analysis of relevant information on the development of the incident and the actions and procedures taken to prevent, contain and recover from the incident, with a view to making adjustments to the business continuity plan as necessary.	

7 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of Financial Technology Institutions Regulatory Law and its General Provision

The National Banking and Securities Commission (CNBV) has issued the *Financial Technology Institutions Regulatory Law* (Fintech Law) and its General Provisions, which provides for services offered by financing institutions and electronic payment institutions. The following section summarizes the control requirements related to cloud service providers in the Fintech Law and its General Provisions and the specific indicators in the Fintech Law and its General Provisions, and describes how HUAWEI CLOUD, as a cloud service provider, helps financial institution customers meet these control requirements.

7.1 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Financial Technology Institutions Regulatory Law (Fintech Law)

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
39	Section I: Authorization	When applying for third-party outsourcing services, FIs are required to obtain authorization from the CNBV Commission and must attach the following materials: 1. Controls and policies regarding operational risk, provide evidence that they provide FIs with secure, reliable and technical support, with minimum security standards to ensure the confidentiality, availability and integrity of information, and to prevent fraud and cyber-attacks. 2. List of agreements or contracts with other ITFs or technical service providers that are necessary to perform activities such as key business processes, database management, etc.	Before applying for third-party outsourcing services, FIs shall provide relevant materials as required by this Act and obtain authorization from the CNBV Commission. HUAWEI CLOUD has obtained many international and industry security compliance certifications, including ISO27001, ISO27017, ISO27018, PCI-DSS, and CSA-STAR, and is audited by a third party every year. If necessary, FIs can apply for copies of audit reports from HUAWEI CLOUD through official channels.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
54	Section II: On the Functioning of Fintech Institutions	1. The contracting out of services by FIs with a third party shall not relieve the financial institution or its directors and employees from their obligations under this Law. 2. The CNBV Commission, through FIs, may request third parties to provide information, including books, records, and documents, regarding the outsourced services it provides.	If FIs sign an outsourcing service with a third party, but cannot outsource legal liabilities, the financial institution or its directors and employees shall bear corresponding responsibilities in accordance with the requirements under this Law. The financial institution shall cooperate with the CNBV Commission to collect relevant information from the financial institution's outsourced service providers. HUAWEI CLOUD will assign dedicated personnel to actively respond to the requirements of financial institution and provide related materials.

7.2 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Secondary Regulatory Requirements of the Financial Technology Institutions Regulatory Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
15	Section II: Technical Infrastructure in Internal Processes	1. FIs should logically or physically isolate networks into domains and sub-networks based on different functions or types of data transmitted, including isolating production environments from development and test environments. 2. FIs should configure security for network security components, taking into account factors such as ports, least privilege principles, media management, access control, manufacturer updates and reconfigurations of factory settings. 3. FIs should establish security mechanisms in their applications to ensure protection against attacks such as code injection, session manipulation, information disclosure, and changes in access rights, including applications provided by third parties.	FIs are responsible for network domain division and network security configuration in accordance with the cyber security control requirements specified in this document. At the same time, FIs should also require and manage third parties based on cyber security requirements of the same level. The initial network architecture design and device selection and configuration of HUAWEI CLOUD are considered. The bearer network adopts various multi-layer security isolation, access control, and border protection technologies for physical and virtual networks, and strictly

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			implements management and control measures to ensure HUAWEI CLOUD security. FIs can use the Virtual Private Cloud (VPC) provided by HUAWEI CLOUD to isolate networks in different regions. VPC can build a private network environment for tenants to isolate different tenants at Layer 3 networks. Tenants can fully control the construction and configuration of their own virtual networks, and configure network ACL and security group rules to strictly control network traffic to and from subnets and VMs. Meets tenants' fine-grained network isolation requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
16	Section II: Technical Infrastructure in Internal Processes	1. FIs shall encrypt personal and sensitive information that they receive, generate, store or transmit. 2. Transaction information protected by established security mechanisms is exempt from encryption. 3. The encryption key shall be in the hands of the CIO of the financial institution.	FIs shall encrypt and manage data that needs to be encrypted, such as personal data, private data, and confidential data, in accordance with their data classification policies and principles. Currently, multiple services, such as **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service (RDS), provide data encryption (server-side encryption) for FIs. These services use high-strength algorithms to encrypt stored data. HUAWEI CLOUD provides the Data Encryption Service (DEW) key management function for FIs to centrally manage keys throughout their lifecycle. Without authorization, no one except FIs can obtain a key to decrypt data, ensuring the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			security of data on the cloud of FIs. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. The hardware security module (HSM) used by HUAWEI CLOUD creates and manages keys for FIs. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, meeting users' data compliance requirements and preventing intrusion and tampering. Even HUAWEI O&M personnel cannot steal the root key of FIs. DEW also allows FIs to import their own keys as their master keys for unified management, facilitating seamless integration and interconnection with existing services of FIs. In addition, HUAWEI CLOUD uses customer master key

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			online redundancy storage, multiple physical offline backups of root keys, and periodic backups to ensure key persistence. For more information, see **HUAWEI CLOUD Security White Paper.** When FIs provide web site services over the Internet, they can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. This section describes how to apply for and configure certificates for websites to implement trusted identity authentication and secure transmission based on encryption protocols. In hybrid cloud deployment and global deployment scenarios of FIs, you can use services such as **Virtual Private Network (VPN)**, **Direct Connect**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(DC) and **Cloud Connect (CC)** provided by HUAWEI CLOUD to implement service interconnection and data transmission security between different regions.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
19	Section II: Technical Infrastructure in Internal Processes	FIs should establish retirement management policies to ensure that information stored in discarded or removed storage parts or physical device storage is not recoverable.	FIs should establish a retirement management policy to delete information stored in storage media that is about to be discarded or removed and ensure that deleted information is not recoverable. After the financial institution confirms to delete data, HUAWEI CLOUD deletes the specified data and all copies of the data. It deletes the index relationship between the financial institution and the data, and clears the data before reallocating storage space such as memory and block storage to ensure that related data and information cannot be restored. If physical storage media are discarded, HUAWEI CLOUD degauss, bends, or breaks data on the storage

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			media to ensure that the data on the storage media cannot be restored.
20	Section II: Technical Infrastructure in Internal Processes	FIs should use tools to detect computer viruses and malicious code in their infrastructure and regularly update their detection policies.	FIs should develop vulnerability management mechanisms, regularly scan key services for vulnerabilities, analyze the scanning results, and fix vulnerabilities. On a quarterly basis, HUAWEI CLOUD organizes internal and third-party assessment organizations to scan vulnerabilities on all systems, applications, and networks of HUAWEI CLOUD. For all known security vulnerabilities, HUAWEI CLOUD evaluates and analyzes each vulnerability, formulates and implements vulnerability fixes or workarounds, verifies the fixes, and continuously tracks and confirms that risks are eliminated or mitigated.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
21	Section II: Technical Infrastructure in Internal Processes	FIs should conduct additional testing of the infrastructure at least every two months or after major changes, security incidents. FIs should develop remediation plans to address vulnerabilities identified in testing and prioritize vulnerabilities based on their severity. Vulnerability remediation plans are the responsibility of the CIO and the financial institution shall develop a remediation plan within 10 working days of the discovery of the vulnerability and submit it to the CNBV Commission.	HUAWEI CLOUD publishes discovered vulnerabilities in products or services on its official website and provides warnings. Customers can view security bulletins to understand the impact scope, handling methods, and threat levels of vulnerabilities. FIs can use **Vulnerability Scan Service (VSS)** of HUAWEI CLOUD to implement functions such as web vulnerability scanning, OS vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks exposed to websites or servers. to implement multi-dimensional security detection for services on the cloud.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
23	Section II: Technical Infrastructure in Internal Processes	Electronic payment institutions should establish procedures and mechanisms to restrict access to physical connection ports and peripheral devices, as well as computer or telecommunications infrastructure, and electronic payment institutions should ensure that third parties also have this policy.	FIs should have physical security mechanisms to manage access to physical devices and specify these requirements in their contractual agreements with third parties. The HUAWEI CLOUD information security environment is managed by zones, and physical environment facilities are defined for each zone (including access control, security post, and video surveillance) and different requirements for equipment access control (including photography equipment, storage media, etc.). In addition, HUAWEI CLOUD formulates and implements data transfer policies and access control policies between regions. The access of management personnel and devices in the HUAWEI CLOUD data center is

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			strictly controlled. Security personnel are deployed at the entrances of the data center campus and buildings for 24 hours to check and restrict and monitor the authorized activities of visitors. The access control system adopts different security policies in different areas and strictly checks the access rights of personnel.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
24	Section II: Technical Infrastructure in Internal Processes	FIs shall establish an enterprise information security management policy, which shall include: 1. Logical access control of infrastructure such as databases, operating systems, and software. 2. Infrastructure account and password management policies. 3. Track and monitor access to systems that store financial institution information, including allowing review of access to financial institution information, operational behavior, invalid access attempts, etc. 4. FIs that do not implement the above measures need to obtain prior authorization from the CNBV Commission and the Banxico.	FIs shall formulate internal security management policies, including infrastructure access control, password management, and log management, in accordance with this Regulation. HUAWEI CLOUD has established an O&M and operation account management mechanism. When O&M personnel access the HUAWEI CLOUD management network to centrally manage the system, they need to use employee IDs and two-factor authentication. All O&M accounts are centrally managed by the LDAP and monitored and automatically audited by the unified O&M audit platform. This ensures the end-to-end management of user creation, authorization, authentication, and permission

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			reclaiming. In addition, RBAC rights management is implemented based on different business dimensions and different responsibilities for the same business. Ensure that personnel in different positions and responsibilities can access only the devices managed by the role. HUAWEI CLOUD has formulated password policies and account and password security management regulations to manage the allocation of secret authentication information. The default password of an account in the new system is changed by the user before the first use. When the user needs to reset the password, the user identity is authenticated. FIs can use the **Identity and Access Management (IAM)** of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI CLOUD to manage user accounts that use cloud resources. In addition to password authentication, IAM also supports multi-factor authentication. FIs can choose whether to enable IAM. If a tenant has a secure and reliable external identity authentication service provider, you can map the federated authentication external user of IAM to a temporary user of HUAWEI CLOUD and access the tenant's HUAWEI CLOUD resources. IAM supports hierarchical and fine-grained authorization. Administrators can plan the permissions to use cloud resources based on users' responsibilities. In addition, administrators can set security policies for users to access cloud service systems,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			such as ACLs, to prevent malicious access from untrusted networks. In addition, **Cloud Trace Service (CTS)** of HUAWEI CLOUD can collect, store, and query operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
26	Section III: General Provisions for Technical Infrastructure	FIs should establish communication encryption mechanisms in accordance with best practices and international standards to ensure that encrypted communication protocols are used to ensure information security in point-to-point communications. FIs should adopt up-to-date, non-vulnerable encryption mechanisms with sufficiently long keys and obtain approval from the Banxico and the CNBV Commission.	FIs should establish mechanisms for secure data transmission in accordance with best practices and international standards. When FIs provide web site services over the Internet, they can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. This section describes how to apply for and configure certificates for websites to implement trusted identity authentication and secure transmission based on encryption protocols. For the hybrid cloud deployment and global deployment of FIs, services such as Virtual Private Network (VPN), Direct Connect (DC), and Cloud Connect (CC) provided by HUAWEI CLOUD can be used. This feature implements

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			service interconnection and data transmission security between different areas. The server-side encryption function integrates the server-side encryption function and the key management function of HUAWEI CLOUD **Data Encryption Workshop (DEW)**. The DEW centrally manages keys throughout the lifecycle. Without authorization, no one except FIs can obtain a key to decrypt data, ensuring the security of data on the cloud of FIs. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. An encryption key used by each storage service to encrypt data can be encrypted by FIs master key stored in the DEW, and the financial institution master key is

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			encrypted by a root key stored in a hardware security module (HSM). A complete secure and trusted key chain is formed. The HSM has passed strict international security certification and is anti-intrusion and anti-tamper. Even HUAWEI O&M personnel cannot steal the root key.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
28	Section III: General Provisions for Technical Infrastructure	When FIs enter into a service outsourcing contract with a third party for the development of an information system, it shall: 1. Document its processes, functions, and configurations, including its development or acquisition methods, as well as its changes, updated records, and a detailed list of each component of the technical infrastructure. Information security control measures shall be implemented at least in the phases of requirement analysis, design, IT system development (purchase), system function verification, pre-release vulnerability testing and code analysis, system change, and security destruction. 2. If the software is developed by a third party, the financial institution shall require verification of its integrity and authenticity at the time of installation. 3. Authentication mechanisms should be included between different components of the financial institution. 4. FIs use electronic signatures to guarantee the integrity and non-repudiation of information, whether it is static or in transit. 5. Manage the users who access the technology infrastructure and their permissions. 6. Encrypted communication protocols are used between different computer systems and components. 7. A static review of the security of the computer system every time it is updated through automated tools.	The financial institution shall specify in the service agreement the quality and safety requirements to be met by the equipment or software provided by the service provider, and the financial institution shall be responsible for the security of the entire life cycle of the equipment or software it owns. HUAWEI's development and testing processes comply with unified system security development management regulations. HUAWEI CLOUD uses systems, processes, and automated platforms and tools to manage the software and hardware lifecycle from end to end. The lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			vulnerability management. HUAWEI CLOUD uses the security requirements identified in the security design phase, penetration test cases from the attacker perspective, and industry standards as check items, develops corresponding security test tools, and performs multiple rounds of security tests before cloud services are released to ensure that cloud services meet security requirements. The test is performed in a test environment that is isolated from the production environment to avoid using production data for testing. If production data is required for testing, anonymization must be performed. After the test is complete, data needs to be cleared.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
33	Section III: General Provisions for Technical Infrastructure	FIs should conduct an assessment or audit of information security controls for the technology infrastructure at least annually. FIs should submit the following documents to the regulator: 1. A report specifying the level of information technology risk for the technology infrastructure. 2. Remediation plans to address high-risk issues. 3. Evidence of the implementation of remedial measures. 4. Evidence of risk relief. FIs should evaluate and audit the technology infrastructure of third-party service providers to which they contract and obtain the following documents: 1. Results of assessments or audits conducted at least once a year prior to the commencement of the provision of services by third parties. 2. Remediation plans to address high-risk issues. 3. Evidence of risk relief. The financial institution shall provide the appropriate documentation when requested by the Banxico and the CNBV Commission.	FIs should establish a risk assessment framework to regularly assess the security of their technology infrastructure, including risks associated with outsourcing arrangements. HUAWEI CLOUD has developed a comprehensive information security risk management mechanism, and periodically conducts risk assessment and compliance review to ensure secure and stable running of HUAWEI CLOUD's cloud environment.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
34	Section III: General Provisions for Technical Infrastructure	FIs hire outside technicians to conduct penetration testing of different systems and applications of the technology infrastructure at least once every two years. The financial institution shall send to the Banxico and the CNBV Commission a report stating the conclusions of the test within 20 working days of the completion of the test. If there are high-risk issues, the financial institution should submit a documented remediation plan to Banxico and CNBV within no more than 20 business days after completion of the penetration test to correct these observations. FIs should re-perform penetration testing no more than two months after the vulnerability has been fixed to verify that their vulnerability has been mitigated. FIs should document in the manual the method of risk classification of test results.	FIs shall perform penetration testing and remediation programs for different systems and applications of the technology infrastructure at least every two years in accordance with these regulatory requirements. The financial institution shall report the results of the penetration tests and the remediation plan to the CNBV Commission in accordance with the requirements of these General Provisions. HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. FIs can also use Vulnerability Scan Service (VSS) of HUAWEI CLOUD to implement functions such as web vulnerability scanning, OS

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks exposed to websites or servers to implement multi-dimensional security detection for services on the cloud. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and supervise notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
40	Chapter 3: Business Continuity	1. Develop, review and update business continuity plans as necessary. 2. Assess compliance with the business continuity plan at least annually and report the results to the governing body and update it as appropriate. 3. Verify the operation of the business continuity plan and the implementation of adequacy tests and report the results of such tests to the regulator at least annually. 4. Develop and submit emergency management methods to regulatory institutions. 5. Develop and submit to regulators a methodology for assessing the quantitative and qualitative impact of an incident. 6. Where FIs enter into an outsourced service contract with a third party, the financial institution shall have documentation demonstrating that the third party meets international standards for business continuity.	FIs should identify their key business processes and develop business continuity plans. The financial institution should test the effectiveness of the business continuity plan at least annually, communicate the results of the test to the governing body, and update the plan on an ongoing basis based on the results of the test and the recommendations of the regulatory body. FIs shall develop methods for assessing the impact of emergencies. In case of emergencies, FIs shall notify the regulatory authorities and explain the causes and impacts of the emergencies. HUAWEI CLOUD has developed a business continuity management system that meets its service characteristics and has obtained the IS022301

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. If FIs need HUAWEI CLOUD to participate in the development and execution of its business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
41	Chapter 4: Common information security and business continuity arrangements	FIs should record events, failures or vulnerabilities discovered in the technology infrastructure, which should include at least information related to discover failures, operational errors, attempted computer attacks and actual attacks, and information of users of the technology infrastructure is lost, extracted, tampered with, lost or improperly used. The information provided should include, at a minimum, the date the incident occurred and a brief description of the incident, its duration, the services affected, the FIs affected and the amounts involved, and the corrective actions implemented. and the relevant information shall be backed up in a manner determined by the financial institution and shall be kept for at least 10 years	FIs shall generate, maintain and periodically review event logs recording user activities, anomalies, errors and information security events, and shall back up the logs in accordance with established rules. The backup information shall be retained for at least 10 years. HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has powerful data storage and query capabilities,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has a dedicated internal audit department that regularly audits O&M process activities. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in different scenarios. Customers can use Object Storage Service (OBS) version control, Volume Backup Service (VBS), Cloud

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Server Backup Service (CSBS) to back up documents, disks, and servers on the cloud.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
42	Chapter 4: Common information security and business continuity arrangements	When an information security incident occurs, the CEO shall 1. Notify the CNBV Commission immediately of the appropriate preliminary assessment of information security incidents by e-mail ifpe@banxico.org.mx and CiberseguridadCNBV@cnbv.gob.mx or by approved means. 2. The financial institution shall report the details of the information security incident to the CNBV Commission via email within 5 working days after confirming the information security incident. 3. Submit the information security incident analysis report and handling measures to the CNBV Commission within 15 working days after the incident ends. 4. If information security involves the extraction, loss, elimination, or alteration of sensitive information or the financial institution suspects that these events have occurred, the customer shall be notified within 24 hours after the information security incident occurs or becomes aware of it.	When an information security incident occurs, the financial institution shall report it to the CNBV Commission in accordance with the requirements of these general provisions. HUAWEI CLOUD has a 24/7 professional security incident response team and corresponding security expert resource pool to respond to incidents. HUAWEI CLOUD formulates security incident grading rules and escalation rules, assigns security incidents based on the impact of security incidents on FIs' businesses, initiates the financial institution notification process based on the security incident notification mechanism, and notifies FIs of the incidents. When a serious security incident occurs, which has or

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			may have a serious impact on a large number of FIs, HUAWEI CLOUD can notify the FIs of the incident information in the shortest possible time. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and assist FIs in meeting regulatory notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
49	Chapter 5: Service Contracts with Third Parties and Entrusted Agents	FIs shall obtain authorization from the CNBV Commission and the Banxico when signing outsourcing service contracts with third parties for the provision of services involving the transmission, storage and processing of personal information or sensitive information. The authorisation application shall contain the following information: 1. Describe the service process to be subscribed in detail. 2. The draft contract for the provision of services, which shall indicate the expected date of conclusion of the contract, the rights and obligations of the financial institution and third parties, including the identification of intellectual property rights used to provide the services, shall be provided in Spanish. and clearly define the obligations to be complied with by the third party: a. Provide data, reports, minutes, minutes, documents, correspondence and other required documents. b. Regulators may enter their offices, premises and other facilities for inspection. c. Notify the financial institution at least 30 calendar days prior to the occurrence of any modification of its corporate purpose by the third party or any other change that may affect the provision of the services which are the subject of the contract. d. Confidentiality of information received, transmitted and processed in	FIs shall identify services provided by third parties that involve the pure possession, storage, and processing of personal or sensitive information, and obtain authorization from the CNBV Commission when contracting out with third parties. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the course of providing the Services. e. If the third party will subcontract the services, it shall notify the financial institution. f. Securely transfer, return and process the information specified in the Contract when the third party ceases to provide the Services. g. Maintain a comprehensive audit log that includes a log of accesses or attempts to access, as well as details of operations or activities performed by users of the technology infrastructure. h. Have access control mechanisms that meet the requirements of FIs. i. Allow FIs to conduct security reviews or provide evidence of reviews. 3. A document that provides the technical infrastructure and describes the communication link information provided by the service provider, including the name of the service provider, bandwidth, and type of service provided. Provide a complete address for each service and the location of the primary and secondary data centers where the information is stored and processed. In the case of cloud computing services, the information specified in Article 50 of these Regulations shall be provided. 4. Allow FIs to maintain detailed records of all transactions in their own infrastructure or in third-party infrastructure in the country to ensure business continuity at all times.	physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. If the customer applies, HUAWEI CLOUD will provide the customer with copies of the information security management system as required. HUAWEI CLOUD has been deployed in multiple countries or regions around the world. HUAWEI CLOUD infrastructure is deployed in multiple regions and AZs around the world. Customers can select services in different regions based on their requirements. When the service agreement terminates, Customers can use the Object Storage Migration Service (OMS) and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		5. When a third party has access to FIs' identity image or biometric information, the third party shall provide evidence that it has controls in place to ensure the confidentiality, integrity and availability of that information. 6. Mechanisms by which FIs detect third-party compliance. 7. Assess the importance of the services provided by the third party and the compliance with the contract and report the results to the regulator (as the case may be) or the audit committee of the financial institution. 8. Evidence that third parties possess and implement personal data protection can be verified, and that FIs can comply with relevant laws and regulations. Where services are processed, provided, or performed wholly or partly outside the national territory, FIs should attach documentation that third parties have taken corresponding measures to protect personal data or that these countries have entered into international agreements with Mexico on such matters. 9. FIs do not affect the continuity of business provided by FIs because of geographical distance and language. 10. FIs develop technical support plans to resolve issues and incidents without taking into account time zone and workday differences. 11. If any authority of the third party's country of origin requests the third party to	Server Migration Service (SMS) provided by HUAWEI CLOUD to migrate content data out of HUAWEI CLOUD. Due to the professionalism, urgency, and traceability of security incident handling, HUAWEI CLOUD has comprehensive security log management requirements, security incident grading and handling process, a 24/7 professional security incident response team, and corresponding security expert resource pool to cope with security incidents. HUAWEI CLOUD adheres to the security incident response principles of quick discovery, quick demarcation, quick isolation, and quick recovery. In addition, the incident leveling standards, response time

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		provide information relating to the services it provides to the financial institution, the third party shall notify the institution as soon as possible in accordance with the law and provide the financial institution with a copy of the information it has provided to that authority. The Banxico and the CNBV Commission will decide on the request for authorization referred to in this Article within 25 working days.	limit, and resolution time limit are updated based on the hazards of security incidents to the entire network and customers. HUAWEI CLOUD will not touch customer data unless it provides necessary services for customers or complies with laws and regulations or binding orders of government agencies. To better protect the personal data of Mexican citizens, HUAWEI CLOUD analyzes its compliance with Mexican privacy laws and regulations. For more information, see HUAWEI CLOUD Compliance with Mexico Privacy Law. HUAWEI CLOUD provides the **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which describe the content and level of the services provided

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
50	Chapter 5: Service Contracts with Third Parties and Entrusted Agents	FIs enter into cloud computing service outsourcing contracts with third parties, and when the third party is a foreign enterprise, services may be interrupted due to orders from foreign authorities. FIs in such situations need to include in their business continuity plans one of the mechanisms shown below to ensure that they will maintain the necessary computing and processing capacity and restore business within two hours of the cloud service interruption. 1. Allow FIs to rely on cloud services provided by other cloud computing service providers in addition to the major cloud computing service providers. 2. The institutions concerned should be allowed to have their own infrastructure.	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If the customer requires HUAWEI CLOUD to participate in the business continuity plan within the organization, HUAWEI CLOUD will actively cooperate with the customer. To provide customers with continuous and stable cloud services, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on customers is considered as an important criterion for determining key services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
51	Chapter 5: Service Contracts with Third Parties and Entrusted Agents	FIs must comply with the following rules when signing service contracts with third parties: 1. The third-party service provider conducts an internal or external audit at least annually, or there is evidence that the contracted third party conducts an audit. 2. Documentation describing the technical infrastructure and information security, including: a. A description of the technical characteristics of the systems, equipment and applications covered by the contract. b. A detailed description of the mechanisms to ensure the transmission and storage of personal information or sensitive information, including the version of the encryption protocol and the security components of the technical infrastructure. c. A description of the types of personal or sensitive information that third parties will store in their equipment or facilities or that they may have access to. d. A description of the mechanisms for controlling and monitoring access to personal or sensitive information, as well as logs, databases and security configurations established for this purpose.	FIs shall enter into service agreements with outsourced service providers as required by these regulatory requirements. HUAWEI CLOUD is regularly audited by professional third-party audit organizations every year, and periodically conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. If the customer applies, HUAWEI CLOUD will provide the customer with copies of the information security management system as required.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
52	Chapter 5: Service Contracts with Third Parties and Entrusted Agents	FIs should have a list of service providers which should include, at a minimum, the following information: FIs should have a list of service providers which should include, at a minimum, the following information. 1. Name of the service provider and company. 2. Name of the legal representative of the service provider. 3. Describe the services contracted with third parties, including data or information stored or processed by third parties, if any. 4. If applicable, system information relating to services provided by third parties, including at least the system name, version and function or purpose. 5. Interfaces with other systems and their purpose, including details of the exchange of information. 6. The full address at which the service is performed and the location of the person responsible for performing the service. 7. If applicable, the full address of the primary data center in which the processing equipment of the Contract System is located. 8. Where applicable, the full address of the standby data center in which the processing equipment is located. 9. The number and date of the notice to obtain the approval of the contract service.	FIs shall develop and maintain a list of its suppliers, which shall include the basic information of the service provider, including the name of the service provider, details of the services provided, etc. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and fulfill regulatory requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 2	Minimum Requirements for Developing a Business Continuity Plan	Before developing a business continuity plan, the financial fund institution should do the following. 1. A risk analysis, i.e.: a. In accordance with the methodology referred to in Article 39 of this regulation, the risks associated with the following factors are considered: human (including fraud, integrity, training), process, technology and external (including external suppliers). b. Identify, assess, monitor and mitigate risks associated with operational processes and data processing and transmission services contracted with suppliers. c. Identify the risks associated with the geographic location of the primary data processing and operations center for the processes identified as critical based on the business impact analysis, so that the secondary data processing and operations center is not exposed to the same risks as the primary data processing and operations center. d. Assess whether it is necessary to establish alternative data processing and operation sites or services which, where appropriate, should be able to operate when required and not be subject to the same risks as the main site. 2. A business impact analysis, i.e.: a. Include all services and processes and identify those	FIs should establish their own business continuity mechanism and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Every year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		services that are critical and considered essential to business continuity, including those contracted with service providers. b. Determine minimum resources (Human, logistical, material, technical infrastructure and resources of any other nature) in order to maintain and rebuild the services and procedures of FIs in the event of an operational emergency and at the end of the emergency. c. Formulate relevant programs related to possible emergency situations, taking into account the following: i. Natural and environmental disasters. ii. Communicable diseases. iii. Cyber-attacks or attacks on computer activities. iv. Vandalism. v. Terrorism. vi. Power supply is interrupted. vii. Failure or unavailability of technical infrastructure (telecommunication, information processing and networking). viii. Inadequate human, material or technical resources. ix. Service provided by a third party is interrupted. d. Assess the quantitative and qualitative impact of the incident based on the scenarios defined for each critical process. e. Define recovery priorities for each critical process.	continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on FIs is considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. FIs can rely on the multi-region and multi-AZ architecture

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		f. Determine Recovery Time Objectives (RTOs) for each service and process. For processes considered critical, the recovery time should not exceed two hours. g. Where appropriate, establish recovery objective points (RPOs) as the maximum tolerable data loss for each critical process. h. Identify and assess risks associated with operational processes and data processing and transmission services contracted with suppliers, as well as risks associated with the custody and security of information of the institution or its FIs. 1. The Business Continuity Plan shall, based on the impact analysis referred to in Section II of this Annex, describe the processes that should be prioritized for recovery in the event of an emergency. 2. The Business Continuity Plan should include, as a minimum, the following actions. a. Prevention, which shall include, at a minimum, the identification of activities and procedures related to: i. Assess the institution's processes and services to reduce the impact of the vulnerability of the processes and services on business continuity. ii. The availability of the necessary human, financial, material, technical and technological infrastructure resources for timely action in the event of an operational emergency.	of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. In addition, as a cloud service provider, HUAWEI CLOUD meets organizations'

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		iii. Establish a program to test the business continuity plan, update it at least annually, and update it in advance if there are significant changes to the institution's technology infrastructure, processes, products and services, or internal organization, and evaluate the business continuity plan. iv. Business Continuity Training Program. v. Procedures for registering, following up, tracking and communicating to relevant personnel the results of testing the business continuity plan. b. Emergency events, which shall include the following: i. Identify in a timely manner the nature of the incident affecting the institution's critical processes. ii. Control the impact of incidents on key processes. c. Restoration to bring the institution's services and procedures back to minimum service levels and eventually to normal. d. Assessment, which should include the collection and analysis of relevant information on the development of the incident and the actions and procedures taken to prevent, contain and recover from the incident, with a view to making adjustments to the business continuity plan as necessary.	requirements for information security and information security management continuity in the event of a disaster. HUAWEI CLOUD provides customers with the Storage Disaster Recovery Service (SDRS) and provides disaster recovery (DR) functions for ECS, EVS disk, and Dedicated Distributed Storage Service (DSS). The SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high data reliability and service continuity. DRS helps protect service applications. It replicates data and configuration information of ECS to the DR site and allows the server where service applications reside to start and run properly from another

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			location when the server is down, improving service continuity.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
Annex 4	Information Security Incident Report	1. Institutional information a. Name of the institution. b. The full name of the Chief Information Security Officer and his/her telephone number and email address. 2. Attach the following information about information security incidents to encrypted digital media a. Information security incident description. b. Affected accounts. c. Status of the affected account (blocked, suspended, or activated). d. Affected network areas (Internet, intranet, management network, etc.). e. Affected System Type (file servers, network servers, mail services, databases, workstations, mobile devices, etc.). f. Operating system (indicate the version). g. Protocols or services of affected components. h. The number of components of the affected system at the institution. i. Application(s) involved (specified version). j. Information about the damaged device (brand, software version, firmware, etc.). k. Impact of information security incidents on services. l. Amount of loss in pesos. m. Amounts recovered in pesos.	FIs shall promptly report information security incidents to the CNBV Commission in accordance with the information security reports required by the general provisions. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and assist FIs in meeting regulatory notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		n. The status of the information security incident (resolved or unresolved). o. Indicate whether the information security incident has been reported to any authority. If so, please indicate the authorization and date. p. The public IP address, email address, or domain name of the source of the attack. q. Communication Protocols Used. r. Websites involved. s. Detected Malware. t. Describe in detail the actions taken to mitigate the information security incident and refer to those responsible for implementing those mitigation actions. u. Describe the results of mitigation measures. v. In subsequent similar cases, action is taken to minimize losses. w. Other information that you believe should be brought to the attention of the CNBV Commission.	

7.3 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions of the Financial Technology Institutions Regulatory Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
61	Section V: Business Continuity Plan	FIs should develop a business continuity plan and appoint a dedicated person to be responsible for the plan. These include: 1. Develop a training plan, implement, continuously update and disseminate the plan. 2. Design and implement a communication policy for the business continuity plan, including timely communication with FIs and the public, with adversaries, with different administrative and operational units of the institution itself, and with the CNBV Commission and other competent authorities depending on the nature of the emergency in question. 3. Inform the CNBV Commission of the status of the emergency by sending an email to the contingencias@cnbv.gob.mx and the supervisionfintech@cnbv.gob.mx or other approved means within 60 minutes of confirming the occurrence of the public emergency and the duration of the event exceeds 30 minutes. 4. Approve the quantitative and qualitative analytical methods submitted by	FIs shall appoint specialists to establish business continuity plans and develop RTO and RPO indicators to ensure the continuity of their key businesses in accordance with the requirements of the General Regulations. HUAWEI CLOUD provides an online HUAWEI CLOUD Service Level Agreement, which specifies the service level and responsibilities of HUAWEI CLOUD. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		the Head of Risk Management in accordance with these provisions.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
62	Section V: Business Continuity Plan	FIs should clarify the responsibilities of employees responsible for risk management of business continuity plans, including: 1. Define and submit to the governing body for approval a methodology for assessing the quantitative and qualitative impact of an incident 2. The effectiveness of the methodology is verified annually, its estimates are compared with the actual situation and revised as necessary. 3. Prepare, review and, where appropriate, update or recommend updating a business continuity plan and submit it to the regulator for approval at least annually or more frequently as the regulator decides 4. Test the functionality and adequacy of the business continuity plan at least annually or in the event of significant changes in the technology infrastructure, processes, products and services or internal organization of the collective financier that could affect the recovery strategy 5. Develop procedures to register, follow up, follow up and disseminate results, events or opinions arising from the tests mentioned in the previous section or from the implementation of the	FIs should specify the employees responsible for business continuity, establish their own business continuity mechanism, and develop RTO and RPO indicators to ensure the continuity of their key businesses. If FIs need HUAWEI CLOUD's participation in running its internal business continuity plan, HUAWEI CLOUD will actively cooperate with the financial institution. To provide continuous and stable cloud services for FIs, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics and has obtained the IS022301 certification. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism. Based on the requirements of this system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery levels of key services. When identifying key services, the impact of service interruption on FIs is

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		plan itself in the event of an emergency to those whose functions are affected by an incident or related to the implementation of the business continuity plan. 6. Report the results of the tests referred to in Section IV of this Article to the Regulatory Authority at least annually 7. Assess the scope and effectiveness of the Business Continuity Plan and report the results to the governing body and the areas responsible for key business processes, identifying adjustments needed to update and strengthen the Plan as necessary. 8. Where FIs enter into a contract with a third party for outsourcing services, the financial institution shall have documentation demonstrating that the third party has a valid certificate of its ability to maintain continuity of service issued in accordance with international standards.	considered as an important criterion for determining key services. To help FIs meet compliance requirements, HUAWEI CLOUD develops recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement disaster recovery and backup of their service systems. Data centers are deployed around the world according to rules. FIs can function as disaster recovery centers for each other. The system automatically transfers applications and data from FIs out of affected areas when compliance policies are met, ensuring business continuity. In addition, HUAWEI CLOUD also deploys a global load balancing scheduling center. Applications of FIs are deployed in the data center in N+1 mode. Even if one data center is faulty, traffic can be balanced to other data centers. In addition, as a cloud service provider, HUAWEI CLOUD provides FIs with cloud

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			services on which their businesses depend. Therefore, in addition to outsourcing interruptions or unexpected terminations caused by force majeure, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide FIs with services. Ensure the operation of FIs. Each year, HUAWEI CLOUD conducts publicity and training on business continuity, and periodically conducts emergency drills and tests to continuously optimize the emergency response mechanism.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
63	Section 6: Information Security	1. Each component of the technology infrastructure is capable of performing the functions stated at the time of its design, development or procurement. 2. Information security issues have been taken into account at all stages of the service lifecycle, including requirement description, design, development, test, and release. 3. FIs should logically or physically isolate networks into domains and sub-networks based on different functions or types of data transmitted, including isolating production environments from development and test environments. 4. FIs should configure security for network security components, taking into account factors such as ports, least privilege principles, media management, access control, manufacturer updates and reconfigurations of factory settings. 5. FIs should test components prior to deployment or change, and do not use production data or introduce unauthorized functions during testing. 6. The applications of FIs should include security mechanisms against attacks or intrusions during execution, such as	FIs shall develop information security management processes and mechanisms for technical infrastructure, including physical security, software lifecycle security management, awareness training, data lifecycle management, access control, vulnerability management, and business continuity management, and ensure that outsourced service providers provide corresponding outsourced services according to the requirements of the general provisions. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD implements end-to-end management over the entire lifecycle of software and hardware through comprehensive

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		code injection, session manipulation, information disclosure, and change of access rights, including applications provided by third parties. 7. Have a license or authorization to use, if applicable. 8. Establish security protection measures such as access control, communication security, and information security management, including: a. Establish a user identification and authentication mechanism to ensure that only authorized users are allowed access. Access control should include exceptional access authorization policies and procedures in special cases. b. For technical infrastructure users with high privileges, such as database and operating system administrators, a privileged account management system shall be established. c. Have password management measures to prevent access by unauthorized users and mandate password changes every 90 days or less, and passwords provided to the Outsourced Service Provider shall be	systems, processes, and automated platforms and tools. The entire lifecycle includes security requirement analysis, security design, secure coding and testing, security acceptance and release, and vulnerability management to ensure that information security is designed and implemented in the information system development lifecycle. HUAWEI CLOUD divides a data center into multiple security zones based on service functions and network security risk levels, and uses physical and logical isolation to improve the self-protection and fault tolerance capabilities of the network against intrusions and internal threats. HUAWEI CLOUD data centers are divided into five key security zones: DMZ, Public Service, Point of Delivery (POD), Object-Based Storage (OBS), and Operations Management (OM). In addition to the preceding network partitions, HUAWEI CLOUD also divides the security levels of different zones and determines different attack surfaces and security risks based on different service functions. For example, the zone directly exposed to the Internet has the highest security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		changed at least annually or immediately when the Outsourced Service Provider ceases to provide services. d. FIs should classify their information in a hierarchical manner and encrypt sensitive information. e. FIs should establish session management mechanisms to automatically close unattended sessions and prevent unauthorized simultaneous use of sessions of the same user identity. f. FIs should establish physical access controls. 9. The technical infrastructure has backup mechanisms and recovery procedures. 10. Maintain complete audit logs, including access to or attempted access to information and operations or activities performed by users of the technology infrastructure, and maintain audit records for three years of components that store critical information. Other audit records are retained for at least six months. 11. FIs should establish information security incident management procedures and designate a team to manage and implement them.	risk. The O&M zone, which has little interaction with the Internet and does not open interfaces to other areas, has the smallest attack surface and is relatively easy to control security risks. For details about security zones, see HUAWEI CLOUD Security White Paper. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. FIs can use the IAM of HUAWEI CLOUD to manage user accounts that use cloud resources. Administrators can plan users' permissions to use

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		12.Conduct annual planning and review of the technology infrastructure and develop an update plan. 13.The technical infrastructure should implement automatic control measures or, in the absence of automatic control measures, compensatory controls to reduce the risk of manual or semi-automatic control procedures. 14.Establish controls to prevent tampering or falsification of assets, books and records. 15.Establish procedures to measure the level of availability of internal and external services and service response times. 16.FIs should centrally collect and monitor logs or other information to automatically detect and intercept possible security incidents or incidents. 17.Establish controls to prevent disclosure of technical infrastructure configuration information, such as IP addresses, firewall rules, and hardware and software version information.	cloud resources based on their work responsibilities and set security policies for users to access cloud service systems, such as access control list (ACL), to prevent malicious access from untrusted networks. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. **Cloud Eye Service (CES)** of HUAWEI CLOUD provides a three-dimensional monitoring platform for Elastic Cloud Server (ECS) and bandwidth resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately understand service resource status. Users can set alarm rules and notification policies to learn about the running status and performance of each service instance. FIs can use Vulnerability Scan Service (VSS) of HUAWEI CLOUD to implement functions such as web vulnerability scanning, OS vulnerability scanning, asset content

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			compliance detection, configuration baseline scanning, and weak password detection to automatically detect security risks that websites or servers are exposed to on the network to implements multi-dimensional security detection for services on the cloud. Financial institution can use the Data Encryption Workshop (DEW) of HUAWEI CLOUD to encrypt data. Currently, multiple services of HUAWEI CLOUD, such as Elastic Volume Service (EVS), Object Storage Service (OBS), and Image Management Service (IMS), provide data encryption (server-side encryption) for FIs. In addition, FIs can centrally manage keys throughout their lifecycle through data encryption services. The hardware security module (HSM) used by HUAWEI CLOUD creates and manages keys for FIs. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, meeting users' data compliance requirements and preventing intrusion and tampering. Even HUAWEI O&M personnel cannot steal the root key of FIs. DEW also allows financial institution to import their own keys as

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			their master keys for unified management, facilitating seamless integration and interconnection with existing services of financial institution. In addition, HUAWEI CLOUD uses customer master key online redundancy storage and multiple physical offline backups of root keys to ensure key persistence. For more information, see HUAWEI CLOUD Security White Paper. When financial institution provides web services over the Internet, it can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. By applying for and configuring a certificate for a Web site, the trusted identity authentication and protocol-based secure transmission of the Web site can be implemented. In hybrid cloud deployment and global deployment scenarios of FIs, services such as Virtual Private Network (VPN), Direct Connect (DC), and Cloud Connect (CC) provided by HUAWEI CLOUD can be used to implement service interconnection and data transmission security between different regions. **Host Security Service (HSS)**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			of HUAWEI CLOUD is a security manager for servers. It provides asset management functions for FIs, including managing and analyzing security asset information such as accounts, ports, processes, web directories, and software. FIs can rely on the multi-region and multi-AZ architecture of HUAWEI CLOUD data center clusters to implement DR and backup of their service systems. HUAWEI CLOUD also provides training services for FIs, including help documents, user manuals, and security implementation guides. For more training services and resources provided by HUAWEI CLOUD for FIs, see "Training Services" on the official website. To meet customers' compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
67	Section 6: Information Security	When an information security incident occurs, the CEO shall 1. Immediately notify CNBV Commission of the appropriate preliminary assessment of information security incidents by e-mail CiberseguridadCNBV@cnbv.gob.mx or approved means. 2. The financial institution shall report the details of the information security incident to the CNBV Commission via email within 5 working days after confirming the information security incident. 3. Submit the information security incident analysis report and handling measures to the CNBV Commission within 15 working days after the incident ends. 4. If information security involves the extraction, loss, elimination, or alteration of sensitive information or the financial institution suspects that these events have occurred, the customer shall be notified within 24 hours after the information security incident occurs or becomes aware of it.	When an information security incident occurs, the financial institution shall report it to the CNBV Commission in accordance with the requirements of these general provisions. HUAWEI CLOUD has a 24/7 professional security incident response team and corresponding security expert resource pool to respond to incidents. HUAWEI CLOUD formulates security incident grading rules and escalation rules, assigns security incidents based on the impact of security incidents on FIs' businesses, initiates the financial institution notification process based on the security incident notification mechanism, and notifies FIs of the incidents. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and implement regulatory notices.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
68	Section 6: Information Security	FIs should record events, failures or vulnerabilities discovered in the technology infrastructure, which should include at least information related to discover failures, operational errors, attempted computer attacks and actual attacks, and information of users of the technology infrastructure is lost, extracted, tampered with, lost or improperly used. The information provided should include, at a minimum, the date the incident occurred and a brief description of the incident, its duration, the services affected, the FIs affected and the amounts involved, and the corrective actions implemented. The relevant information shall be backed up in a manner determined by the financial institution and shall be kept for at least 10 years.	FIs shall generate, maintain and periodically review event logs recording user activities, anomalies, errors and information security events, and shall back up the logs in accordance with established rules. The backup information shall be retained for at least 10 years. HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has a dedicated internal audit department that regularly audits O&M process activities. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in different scenarios. Customers can use Object Storage Service (OBS) version control, Volume Backup Service (VBS), Cloud Server Backup Service (CSBS) to back up documents, disks, and servers on the cloud.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
86	Chapter 8: Outsourcing Services to Third Parties	FIs should attach the following to their application for authorization to contract with third parties: 1. The draft contract for the provision of services, which shall state the expected date of conclusion of the contract, the rights and obligations of the financial institution and third parties, including the identification of intellectual property rights used to provide the services, shall be provided in Spanish. 2. In the course of the audit: a. Provide data, reports, records, documents, correspondence and other required documents. b. Regulators may enter their offices, premises and other facilities for inspection. c. If the third party will subcontract the services, it shall notify the financial institution. d. Maintain a comprehensive audit log that includes detailed information on accesses or attempted accesses and operations or activities performed by users of the technology infrastructure. e. Allow FIs to conduct security reviews or	FIs shall identify services provided by third parties that involve the pure possession, storage, and processing of personal or sensitive information, and obtain authorization from the CNBV Commission when contracting out with third parties. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. If the customer applies, HUAWEI CLOUD will provide the customer with copies of the information security management system as required.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		provide evidence of reviews. 3. A document that provides the technical infrastructure, describing the information about the communication link to the service provider, including the name of the service provider, bandwidth, and type of service provided. a. Provide a complete address for each service and the location of the primary and secondary data centers where the information is stored and processed. In the case of cloud computing services, the information specified in Article 50 of these Regulations shall be provided. b. Interrelationship schemes for third-party applications or systems, including the financial institution's own systems. c. Business continuity mechanisms for contractual services. 4. FIs should provide additional descriptions of cloud computing services, including: a. The type of cloud, whether public, private, or hybrid. b. The specific area where the information will be stored and processed.	HUAWEI CLOUD has been deployed in multiple countries or regions around the world. HUAWEI CLOUD infrastructure is deployed in multiple regions and AZs around the world. Customers can select services in different regions based on their requirements. When the service agreement terminates, Customers can use the Object Storage Migration Service (OMS) and Server Migration Service (SMS) provided by HUAWEI CLOUD to migrate content data out of HUAWEI CLOUD. Due to the professionalism, urgency, and traceability of security incident handling, HUAWEI CLOUD has comprehensive security log management requirements, security incident grading and handling process, a 24/7 professional security incident response team, and corresponding security expert resource pool to cope with security incidents. HUAWEI CLOUD adheres to the security incident response principles of quick discovery, quick demarcation, quick isolation, and quick recovery. In addition, the incident leveling standards, response time limit, and resolution

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		c. Describe the control mechanisms that will be used to ensure the confidentiality, integrity, and availability of sensitive information in a public cloud or virtualization scheme that shares infrastructure with other FIs. 5. The Banxico and the CNBV Commission will decide on the request for authorization referred to in this Article within 25 working days.	time limit are updated based on the hazards of security incidents to the entire network and customers. HUAWEI CLOUD will not touch customer data unless it provides necessary services for customers or complies with laws and regulations or binding orders of government agencies. To better protect the personal data of Mexican citizens, HUAWEI CLOUD analyzes its compliance with Mexican privacy laws and regulations. For more information, see HUAWEI CLOUD Compliance with Mexico Privacy Law. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which describe the content and level of the services provided and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
87	Chapter 8: Outsourcing Services to Third Parties	FIs enter into outsourcing services agreements with third parties under the terms permitted by the CNBV Commission, subject to the following terms: 1. Third parties providing services related to the operational processes and management of databases and computer systems agree to the provisions of Article 86 and retain their respective contracts. 2. The financial institution conducts an internal or external audit of the contracted services at least annually, or if there is evidence that the contracted third party conducts an audit. 3. At a minimum, the financial institution maintains at its headquarters documents and information relating to the evaluation, audit findings and, where applicable, the corresponding remediation plan, as well as performance reports of third parties providing the services. 4. FIs shall establish change management and update relevant documents when systems, equipment and applications provided by third parties or their technical features are modified. 5. With regard to technical infrastructure and information security, the	FIs shall establish contracts and user agreements as required by these regulatory requirements. HUAWEI CLOUD has also developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		following documents are also required: a. Description of the technical characteristics of the third party's systems, equipment and applications. b. Details the mechanisms for encrypted transmission and storage of information, if applicable. c. Details including the type of information of collective financiers and FIs, including a description of the type of sensitive information that third parties will store in their equipment or facilities. d. Mechanisms for monitoring access to sensitive information in the system, as well as log management and security configuration mechanisms established for this purpose.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
88	Chapter 8: Outsourcing Services to Third Parties	FIs should have a list of service providers which should include, at a minimum, the following information. 1. Name of the service provider and company. 2. Name of the legal representative of the service provider. 3. Describe the services contracted with the third party, including the data or information stored or processed by the third party, if any. 4. If applicable, system information relating to services provided by third parties, including at least the system name, version and function or purpose. 5. Interfaces with other systems and their purpose, including details of the exchange of information. 6. The full address at which the service is performed and the location of the person responsible for performing the service. 7. If applicable, the full address of the primary data center in which the processing equipment of the Contract System is located. 8. Where applicable, the full address of the standby data center in which the processing equipment is located.	FIs shall develop and maintain a list of its suppliers, which shall include the basic information of the service provider, including the name of the service provider, details of the services provided, etc. HUAWEI CLOUD will cooperate with FIs to provide relevant reporting materials and fulfill regulatory requirements.

8 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Insurance and Guarantee Institution Law and its General Provisions

Mexico's National Insurance and Bonding Commission (CNSF) has issued the *Insurance and Guarantee Institution Law* and its General Provisions, which are specific to the management and operation of insurance institutions, guarantee institutions and mutual insurance companies.

8.1 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the Insurance and Guarantee Institution Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
268	Section IX: Investments in Other Companies and Procurement of Services from Third Parties	FIs must comply with the following regulations when signing outsourced business service contracts with third parties: 1. Comply with the technical and operational guidelines relating to the services provided, as well as the relevant provisions guaranteeing the confidentiality of the information of the users of the banking system in the provision of the services. 2. FIs shall establish requirements for operating and controlling procedures for the provision of services by third parties. 3. FIs shall establish monitoring procedures and policies to ensure that third parties' performance of contracts is monitored, including the obligation of third parties to provide records, information and technical support related to the services as requested by the CNBV Commission and the institution's external auditors. 4. The CNBV Commission and FIs shall have the right to audit, supervise and monitor third party service providers at any time, and the FIs shall be obliged to provide relevant	FIs should specify security control requirements for services provided by third parties in contracts signed with third parties, and develop third-party performance monitoring policies to monitor the fulfillment of service contracts by third parties. HUAWEI CLOUD provides the **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specify the service content and service level, and responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		reports to the CNBV Commission. The CNBV Commission may issue an opinion or corrective action to FIs based on the results of an audit of a third party. 5. Managers and employees of third parties, as well as ex-employees, shall also comply with the provisions of this Article. 6. FIs may not agree to businesses and services provided exclusively by third parties. 7. In the event of failure by FIs to comply with this provision or which may affect the continuity of the credit institution's business or the protection of the public interest, the CNBV Commission may, after the institution has been granted the right to a hearing, order a partial or total, temporary or final suspension of services or commissions provided through the third party concerned.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
269	Section IX: Investments in Other Companies and Procurement of Services from Third Parties	1. The contracting of outsourced services by FIs with a third party shall not relieve the financial institution or its directors and employees of the obligation to comply with the provisions of this Act and the general provisions arising therefrom. 2. The CNBV Commission, through FIs, may request third parties to provide information, including books, records and documents, on the provision of outsourced services by them.	If FIs sign an outsourcing service with a third party, but cannot outsource legal liabilities, the financial institution or its directors and employees shall bear corresponding responsibilities in accordance with the requirements under this Law. The financial institution shall cooperate with the CNBV Commission to collect relevant information from the financial institution's outsourced service providers. HUAWEI CLOUD will assign dedicated personnel to actively respond to the requirements of financial institution and provide related materials.

8.2 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of the General Provisions Applicable to the Insurance and Guarantee Institution Law

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
3.6.3	Section 3.6: Procurement of Services from Third Parties	When FIs sign a service outsourcing contract with a third party, it should consider: 1. The third party institution has the necessary technical, financial, administrative and legal experience and capacity to perform the corresponding services. 2. Establish business continuity and contingency plans to deal with emergencies caused by third parties. 3. Define database management responsibilities and require confidentiality and security of relevant information. 4. Determine whether the third party has an internal control system and require the third party to receive regular training. 5. Limit the possibility of subcontracting services by third parties.	FIs should include the requirements in their contracts with third parties. FIs should establish criteria for the selection of third-party service providers and mechanisms for monitoring third-party performance and contract performance. HUAWEI CLOUD provides the HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.16	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	Institutions that use electronic means to perform operations and provide services shall adopt security measures or mechanisms for the transmission, storage and processing of information through such electronic means to prevent it from becoming known to third parties. To this end, institutions shall comply with the following provisions: 1. Encrypt or use encrypted means of communication during the transmission of sensitive user information (e.g., passwords, personal identification number (PIN), any other authentication factors) processed electronically. 2. FIs should ensure that encryption keys and encryption and decryption systems are installed in highly secure devices, such as HSM (Hardware Security Module), and that management measures are in place to prevent unauthorized access and disclosure.	FIs should manage their information assets in a unified manner, define the owner of the information assets, and establish security control measures throughout the data lifecycle. When FIs provide web site services over the Internet, they can use the certificate management service provided by HUAWEI CLOUD and world-renowned certificate providers. This section describes how to apply for and configure certificates for websites to implement trusted identity authentication and secure transmission based on encryption protocols. For the hybrid cloud deployment and global deployment of FIs, services such as **Virtual Private Network (VPN)**, **Direct Connect (DC)**, and **Cloud Connect (CC)** provided by HUAWEI CLOUD can be used. This feature implements service interconnection and data transmission security between different areas. The server-side encryption function integrates the server-side encryption function and the key management function of HUAWEI CLOUD **Data Encryption Workshop (DEW)**. The DEW centrally manages keys throughout the lifecycle. Without authorization, no one except FIs can obtain a key to decrypt data, ensuring the security of data on the cloud of FIs. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. An encryption key used by each storage service to encrypt data can be encrypted by FIs

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			master key stored in the DEW, and the financial institution master key is encrypted by a root key stored in a hardware security module (HSM). A complete secure and trusted key chain is formed. The HSM has passed strict international security certification and is anti-intrusion and anti-tamper. Even HUAWEI O&M personnel cannot steal the root key.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.17	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	FIs shall comply with the following regulations when establishing access control for databases, files, and storage media. 1. Allow access to databases and documents only to authorized personnel of the institution and record the details of each visit. 2. The remote access channel should use the encryption mechanism. 3. Develop security procedures to destroy storage media containing sensitive user information. 4. Develop policies relating to information transmitted and received by electronic means and verify compliance with those policies by third parties. 5. Unauthorized access will be held legally liable, including third parties providing services to FIs.	FIs shall establish a user access management mechanism to restrict and supervise access to the system. HUAWEI CLOUD has built an information security management system based on ISO27001 and formulated an overall information security policy for HUAWEI CLOUD, which specifies the structure and responsibilities of information security management organizations, management methods of information security system documents, and key directions and objectives of information security, including: asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. FIs can use the IAM of HUAWEI CLOUD to manage user accounts that use cloud resources. Administrators can plan users' permissions to use cloud resources based on their work responsibilities and set security policies for users to access cloud service systems, such as access control list (ACL), to prevent malicious access from untrusted networks. **Cloud Trace Service (CTS)** of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. **Cloud Eye Service**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(CES) of HUAWEI CLOUD provides a three-dimensional monitoring platform for Elastic Cloud Server (ECS) and bandwidth resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately understand service resource status. Users can set alarm rules and notification policies to learn about the running status and performance of each service instance. To cooperate with customers to meet compliance requirements, HUAWEI CLOUD has established an O&M and operation account management mechanism. When O&M personnel access the HUAWEI CLOUD management network to centrally manage the system, they need to use employee IDs and two-factor authentication. All O&M accounts are centrally managed by the LDAP and monitored and automatically audited by the unified O&M audit platform. This ensures the end-to-end management of user creation, authorization, authentication, and permission reclaiming. In addition, RBAC rights management is implemented based on different business dimensions and different responsibilities for the same business. Ensure that personnel in different positions and responsibilities can access only the devices managed by the role. After the financial institution confirms to delete data, HUAWEI CLOUD deletes the specified data and all copies of the data. It deletes the index relationship between the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			financial institution and the data, and clears the data before reallocating storage space such as memory and block storage to ensure that related data and information cannot be restored. If physical storage media are discarded, HUAWEI CLOUD degauss, bends, or breaks data on the storage media to ensure that the data on the storage media cannot be restored.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.18	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	1. If sensitive information in the custody of a brokerage firm or a third party providing services to it is extracted, lost, or if the brokerage firm suspects unauthorized access to such information, the general manager or his designated staff shall report in writing to the CNBV Commission within 5 calendar days of the occurrence of the relevant event. 2. The Brokerage Company shall immediately investigate the causes leading to the deletion, loss, or unauthorized access of sensitive information, and the results, progress, and improvement measures of the investigation shall be sent to the CNSF Commission within three months after the occurrence of the incident. 3. Within three working days after the occurrence or knowledge of the event, notify the customer of the possible information extraction, loss, or illegal acquisition through the notification method	FIs shall develop a data breach response process in accordance with the requirements of this General Provision. The process shall include requirements and steps for notifying and reporting stakeholders, such as data controllers, data subjects, and regulatory authorities, and how to respond to data breaches caused by suppliers. To help FIs meet the requirements of reporting data loss and breach incidents to stakeholders, HUAWEI CLOUD has set up a 24/7 professional security incident response team and expert resource pool to promptly disclose related incidents and notify FIs in accordance with laws and regulations.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		specified by the customer. 4. Notify the audit committee and risk committee of the brokerage firm as soon as the event is verified.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.20	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	FIs should record events, failures or vulnerabilities discovered in the technology infrastructure, which should include at least information related to discover failures, operational errors, attempted computer attacks and actual attacks, and information of users of the technology infrastructure is lost, extracted, tampered with, lost or improperly used. The information provided should include, at a minimum, the date the incident occurred and a brief description of the incident, its duration, the services affected, the FIs affected and the amounts involved, and the corrective actions implemented. The relevant information shall be backed up in a manner determined by the financial institution and shall be kept for at least 10 years.	FIs shall generate, maintain and periodically review event logs recording user activities, anomalies, errors and information security events, and shall back up the logs in accordance with established rules. The backup information shall be retained for at least 10 years. HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has a dedicated internal audit department that regularly audits O&M process activities. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating. HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in different scenarios. Customers can use Object Storage Service (OBS) version control, Volume Backup Service (VBS), Cloud

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Server Backup Service (CSBS) to back up documents, disks, and servers on the cloud.
4.10.21	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	1. FIs shall establish a log audit system, including: a. Records of access to information; b. Access time. 2. The logs of FIs should be stored for at least 180 calendar days, and mechanisms to prevent tampering and access control procedures should be established. 3. Institutions must periodically review the logs referred to in this section and report any unusual events to the Audit Committee and the heads of risk management areas if they identify them.	FIs should establish a user access management mechanism to restrict and monitor access to the system, and regularly audit logs. HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has a dedicated internal audit department that regularly audits O&M process activities. Cloud Trace Service (CTS) of HUAWEI CLOUD collects, stores, and queries operation records of various cloud resources. CTS can be used in common application scenarios, such as security analysis, compliance audit, resource tracing, and problem locating.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.23	Section 4.10 Provisions on the use of electronic means to conclude insurance and secured transactions	FIs should establish an infrastructure review system, which should clearly specify: 1. Review at least annually or whenever there are significant changes to such infrastructure, including at least: a. User authentication mechanism. b. Infrastructure configuration and access control. c. Updates required for operating system and software. d. Vulnerability analysis of infrastructure and systems. e. Identification of possible unauthorized modifications to the original software. f. Technical infrastructure, systems and processes related to electronic media. g. System analysis of critical applications related to e-services to identify erroneous, unauthorized functions.	FIs shall establish an infrastructure review system in accordance with the requirements of these General Provisions. HUAWEI CLOUD has a dedicated audit team to periodically evaluate the compliance and effectiveness of policies, procedures, and related measures and indicators. In addition, independent third-party assessors provide independent assurance by performing periodic security assessments and compliance audits or inspections (e.g. SOC, ISO standards, PCIDSS audit) to assess the security, integrity, confidentiality, and availability of information and resources for an independent assessment of risk management content/ processes. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by the customer.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		2. FIs shall use automated means to detect and prevent incidents and unauthorized access that may affect the confidentiality, integrity and availability of user information.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
12.1.6	Section 12.1: Procurement of services with third parties	FIs must specify in their outsourced service contracts with third parties: 1. Ownership of information, confidentiality clauses, and liability clauses. 2. Intellectual property rights. 3. Mechanisms for verifying compliance with the terms of the contract. 4. Third-party contingency plans. 5. Third-party training programs. 6. Technical, operational, control procedures and laws and regulations that the third party must comply with. 7. Third parties shall accept: a. Access to the physical premises of the outsourced service provider by the receiving institution's external auditors, by the CNSF Commission or by a third party designated by the CNSF Commission itself to verify that the services or entrustments provided by the institution allow the latter to comply with the	FIs should establish contracts with third parties in accordance with relevant requirements. HUAWEI CLOUD has developed an offline contract template, which can be customized based on the requirements of FIs. HUAWEI CLOUD may modify or terminate the service or modify or remove the functions of the service at any time. If there is a material change or discontinuation of the services to which you subscribe, we will notify you by posting a notice on our website or otherwise.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		legal requirements applicable to it. b. Provide systems, records, manuals, and documents related to the services to the Institution's own external auditors and the CNSF Commission or its designated third parties, at the institution's request. It should also allow the responsible person to have access to offices and facilities related to the services provided. c. Notify the Institution at least 45 calendar days in advance of any change in the corporate purpose or internal organization of the third party service provider that may affect the provision of the services covered by the contract.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
12.1.7	Section 12.1: Procurement of services with third parties	The financial institution must determine before entering into a contract whether the third party has the relevant experience, technical, financial, administrative and legal capacity, as well as the material, financial and human resources necessary to ensure reliability and security in the provision of such services.	FIs should conduct due diligence to ensure the reliability and security of third-party service providers before selecting service providers. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements and due diligence initiated by the customer. **Technical Capabilities:** HUAWEI CLOUD provides cloud services online to open up HUAWEI's 30-year technical accumulation and product solutions in the ICT infrastructure field to FIs. HUAWEI CLOUD has five core technical advantages: full-stack, all-scenario AI, multi-architecture, ultimate performance, security and reliability, and openness and innovation. For example, in the AI field, HUAWEI CLOUD AI has been implemented in more than 300 projects in 10 industries, including cities, manufacturing, logistics, Internet, healthcare, and campus. In terms of diversified architectures, HUAWEI CLOUD has built a new architecture of cloud services based on x86, Kunpeng, and Ascend. This architecture enables various applications to run on the most appropriate computing capabilities and maximizes the value of FIs. **Financial Situation:** HUAWEI CLOUD is HUAWEI's cloud service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. **Business Reputation:** As always, HUAWEI CLOUD

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			adheres to the "financial institution-centricity", which has led more and more FIs to choose HUAWEI CLOUD. HUAWEI CLOUD has made major breakthroughs in multiple industries in China, such as the Internet, VOD live broadcast, video surveillance, genetics, and automobile manufacturing. **Corporate Culture and Service Policies Applicable to FIs:** HUAWEI CLOUD defines product security and function requirements based on FIs' business scenarios, laws, regulations, and regulatory requirements during product and service planning and phases, and implements functions in the R&D design phase to meet FIs' requirements. Based on industry requirements and rich cloud services, HUAWEI CLOUD releases financial industry solutions to provide end-to-end cloud solutions for FIs such as banks and insurance.
12.1.9	Section 12.1: Procurement of services with third parties	Policies and standards approved by the financial institution's board of directors must provide for the possibility of audit of third parties.	FIs should set out audit requirements and procedures for third-party service providers in their systems and obtain approval from the Board of Directors. HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements initiated by FIs. FIs' rights and interests in auditing and monitoring HUAWEI CLOUD will be promised in agreements signed with FIs based on actual situations.
12.1.10	Section 12.1: Procurement of services with third parties	Third-party outsourced service providers must be subject to the CNSF Commission's inspection and oversight of FIs and the services they contract with.	

9 Conclusion

This document helps customers understand HUAWEI CLOUD's compliance with the regulatory requirements of the Mexican financial industry, This aims to help customers learn more about HUAWEI CLOUD's compliance status with Mexico’s regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this document also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of the Mexico’s financial industry on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

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

10 Version History

Date	Version	Description
December 2021	1.0	First release

