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

Issue 2.1

Date 2024-08-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview

1.1 Background and Purpose of Publication

Following the recent wave of technological development, more and more FIs (Financial Institutions) are planning to transform their business by leveraging high-technology to reduce costs, improve operational efficiency and innovate. To regulate the application of Information Technology (IT) in the financial industry, Central Bank of Argentina (BCRA) has put forward a series of regulatory requirements, guidelines and notices on how Argentine FIs conduct technology risk management and technology outsourcing management.

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

1.2 Introduction of Applicable Financial Regulatory Requirements in Argentina

BCRA is the main financial supervisory body in Argentina, responsible for the regulation, inspection and supervision of FIs in Argentina. Superintendency of Financial and Exchange Entities (SEFyC) under the BCRA is responsible for tracking, monitoring, analysis, auditing, and compliance inspections of Argentine FIs.

BCRA issued COMMUNICATION "A" 6375 ("A" 6375 for short) on November 17, 2017. This regulation puts forward relevant management requirements for FIs that use decentralized/outsourcing services. The agency provides guidance on risk management for decentralization/outsourcing activities.

Note: BCRA issued COMMUNICATION "A" 4609" ("A" 4609 for short) on August 29, 2018. This regulation defines the main requirements that FIs need to comply with in scenarios such as information assets, data processing, operating procedures, record storage, database management, system changes, event management, technical documentation, and compliance. But at the same time, considering that the requirements in all scenarios in "A" 4609 are reflected in "A" 6375, Moreover, the requirements stipulated in "A" 6375 are more comprehensive and specific, so this guidance will focus on the regulatory requirements of "A" 6375.

BCRA issued COMMUNICATION "A" 6354 ("A" 6354 for short) on November 3, 2017, and later BCRA amended it, and issued "A" 6375 on November 17, 2017, to complete the requirements that FIs need to follow when decentralizing/outsourcing IT services to service providers.

BCRA issued COMMUNICATION "A" 7266 ("A" 7266" for short) on April 16, 2021. This regulation establishes guidelines for financial institutions in cyber incident response and recovery, with the aim of protecting financial market stability and providing ecosystem-wide cyber resilience.

1.3 Definitions

- **HUAWEI CLOUD**

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

- **Customer**

  Registered users having a business relationship with HUAWEI CLOUD.

- **Outsourcing**

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

- **Service provider**

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

- **Cloud computing**

  Means a type of internet-based computing that provides shared computer processing resources and data on demand according to the definition by the National Institute of Standards and Technology (NIST).

2 HUAWEI CLOUD Security and Privacy Compliance

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

HUAWEI CLOUD has attained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure 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.
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.

Certification	Description
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 EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
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

Certification	Description
	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.
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

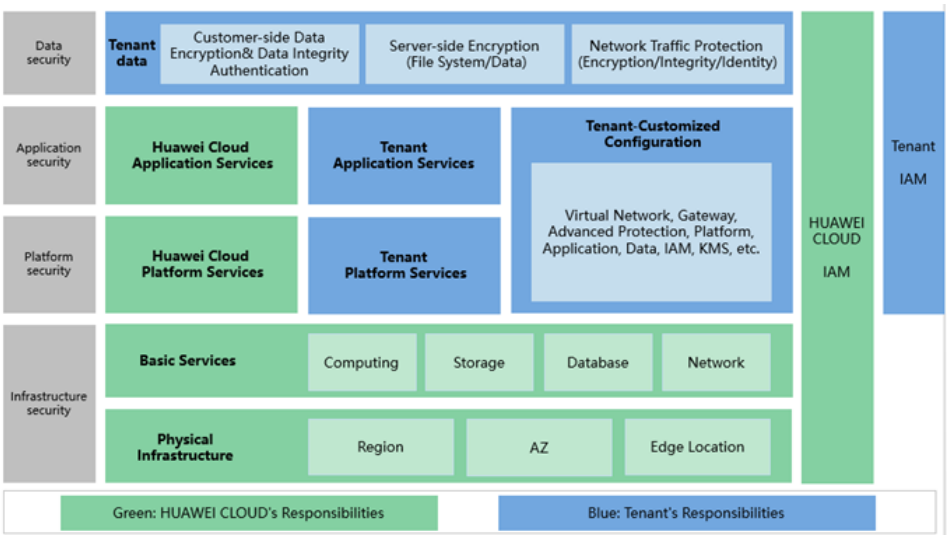
Certification	Description
	organization.
Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management 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.
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 privacy protection 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 Data 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 the Requirements of BCRA “A”6375

"A" 6375 defines the regulatory requirements that FIs need to follow when outsourcing IT services to third-party service providers (including cloud service providers) and the matters that need to be handled when outsourcing business.

When FIs are seeking to comply with the requirements provided in the "A" 6375, 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 "A" 6375, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

5.1 Notifications and conditions

Section 2 of “A” 6375 requires FIs to notify the supervisory body in advance and meet certain conditions when decentralizing and/or outsource activities. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.1	Requirement of prior notice	FIs may decentralize and/or outsource activities that do not consist in serving customers and/or the general public (administration, IT services, filing, printing, etc.) according to the following scheme, prior notice given to the SEFyC at least 60 calendar days prior to the date of commencement of such activities.	When FIs decentralizes/outsources activities that are not part of their customers and/or the public, FIs should notify the SEFyC 60 days prior to the commencement of such activities. HUAWEI CLOUD will provide relevant information to help FIs implement notification activities
2.2	Requirement of prior notice	Decentralized and/or outsourced activities should observe the following conditions: • Comply with the technical	FIs should identify technical and regulatory requirements related to decentralized and/or outsourced activities and specify these requirements in service agreements

		regulations corresponding to the nature and type of activities, the outsourcing contract or decentralization service agreement shall expressly stipulate the relevant technical and regulatory requirements, the requirements of periodically audit by SEFyC. • FIs must define a Unified Access Point to exercising active, continuous, permanent control and monitor all IT outsourcing activities and data of FIs. • The agents to whom Information Technology Services are decentralized or outsourced must undertake to carry out internal audits, at least on an annual basis, with respect to the decentralized/outsourced activities, and must submit to the General Management of FIs the reports of such audits. The reports of such audits must be sent to the Systems External Audit Management. In addition, they must submit the external auditors' reports on their reviews of decentralized/outsourced activities. FIs and third parties contracted by them must accept agents appointed by SEFyC to perform their supervisory functions.	signed with third parties. FIs should also require service providers to conduct internal audit and external audit on decentralized and/or outsourced activities at least once a year in the service agreement, and clarify that SEFyC has the right to supervise service providers. FIs must implement a Unified Access Point to exercising active, continuous, permanent control and monitor all IT outsourcing activities and data of FIs. Huawei Cloud comply with the requirements agreed in the agreements signed with FIs, and will arrange special personnel to actively cooperate with the FIs and financial transaction entity supervision (SEFyC)/ the agents designated by the supervision to audit and supervise Huawei Cloud. FIs' rights and interests in auditing and supervising Huawei Cloud will be promised in the agreement signed with FIs according to the actual situation. In addition, Huawei has established a dedicated security audit team to review compliance with global security laws and regulations and internal security requirements. Huawei has set up a dedicated security audit team to periodically review compliance with security laws and regulations worldwide as well as internal security requirements. The team dedicates over ten members to perform a two-month long annual audit on Huawei Cloud operations worldwide, paying close attention to such Huawei Cloud aspects as legal, regulatory, and procedural compliance; business goal and milestone accomplishment; integrity of decision-making information; and security O&M risks. Audit results are reported to Huawei's Board of Directors and executive management, who ensure that any and all identified issues are properly resolved and closed. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC,

			CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. If necessary, FIs can apply to HUAWEI CLOUD through official channels to obtain copies of audit reports.
2.3	Communication requirements	When FIs communicate decentralization/outsourcing activities with the SEFyC, the communication must include the following information: • The nature of each activity covered. • The domicile where the activities will be carried out or in which the control environment for the administration and operation of the information technology and information systems will be established. • The starting date of the decentralized implementation of the activities. • If the activities are outsourced to a third party, a copy of the outsourcing contract must also be attached. • Decentralized and/or outsourced activities will be subject to the technical regulations corresponding to the nature and type of activities. • The outsourcing contract or decentralization service agreement shall expressly stipulate that the participating parties accept and comply with the relevant technical regulatory requirements, The power of SEF&C to periodically audit compliance with these conditions. • Signed in all cases by a person with sufficient authority to do so.	FIs should notify the SEFyC as required by regulations, and submit materials such as a list of information related to decentralized activities and a copy of the outsourcing contract. HUAWEI CLOUD will provide relevant information to help FIs implement notification activities

		The required documentation must be sent through the modality established by SEF&C in "pdf" format file, being the originals kept in the financial entity at SEF&C's disposal. The legal representative of the entity must state by means of a sworn statement that all the documentation sent by electronic means is a true copy of the documentation kept by the entity and is at the disposal of the SEF and C, detailing the place where it is kept.	

5.2 Unified Access Point (PAU)

Section 7.3 of “A” 6375 requires FIs to define a unified access point through which FIs can control and monitor IT outsourcing activities and data. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.3	Unified Access Point	FIs must define a Unified Access Point to exercising active, continuous, permanent control and monitor all IT outsourcing activities and data of FIs.	FIs in Argentina should define a Unified Access Point through which to control and monitor all IT outsourcing activities and data. HUAWEI CLOUD provides **Identity and Access Management (IAM)** for FIs to manage their accounts that use cloud resources. FIs can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. In addition, the **Cloud Eye Service (CES)** provides users with a three-dimensional monitoring platform for **Elastic Cloud Server (ECS)**, bandwidth, and other resources. CES provides real-time monitoring

			alarms, notifications, and personalized report views to help accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.

5.3 Security processes

Section 7.2 of "A" 6375 requires FIs to formulate security processes and contents in seven areas. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.2	Security processes	FIs and service providers are required to have detailed security processes and contents in the following 7 areas: • Information Security Governance (ISG) • Awareness and Training (AT) • Access Control (CA) • Integrity and Registration (IR) • Monitoring and Control (MC) • Incident Management (IM) • Continuity of Operations (CO) FIs are required to report BCRA of their IT organizational structure, operational structure, and security responsibility sharing model with service providers.	FIs should formulate detailed security procedures and contents in the 7 required areas, and inform BCRA of information such as its IT organizational structure, operational structure and security responsibility sharing model with service providers. HUAWEI CLOUD clearly defined a security responsibility sharing model with FIs. Please refer to ***White Paper for HUAWEI CLOUD Data Security*** for details of the responsibility sharing model. HUAWEI CLOUD will also actively cooperate with FIs to implement the reporting to BCRA. In addition, according to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security,

			system development security, supplier management, information security incident management, and business continuity, etc.

5.4 Scenario Matrix

Section 7.5 of "A" 6375 outlines a "scenario matrix", which describes four different IT outsourcing scenarios according to the nature of data processed, data types and outsourcing service categories involved, and BCRA summarizes the minimum technical operation requirements for each scenario. The following table summarizes the scenario matrix, and the specific technical operation requirements corresponding to the numbers are detailed in Section 5.5 of this document:

Stage	Situation	Information Security Government	Awareness and Training	Access Control	Integrity and Registration	Monitoring and Control	Incident Management	Continuity of Operations
ESD001	Customer data: use/exploitation, conservation and transportation, including financial transactions including customer data.	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD002	Financial accounting data: use/exploitation, retentio	RGS001 RGS002 RGS003 RGS004	RCC001 RCC002 RCC005 RCC006	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

	n and transport, including or not data.	RGS005 RGS006 RGS007	RCC007 RCC008 RCC010 RCC012 RCC013		RIR021 RIR022 RIR023 RIR024			
ESD003	Financial transactional data: use/exploitation, conservation and transport that does not include customer data.	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD004	Operational data: use/exploitation, conservation and transport that does not incl. accounting financial information, customer or transaction-	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023 RIR025	RMC003 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

	financial year.							

5.5 Technical-operational requirements

Chapter 7.7.1 of "A" 6375 requires FIs to meet the technical operational requirements of Information Security Government. The relevant control requirements and HUAWEI CLOUD's responses are as follows.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.1	Information Security Government technical-operational requirements	RGS001:FIs /providers should define complete, exhaustive and clear IT service-related roles, responsibilities, and the sharing of responsibilities between FIs and service providers, comply with the principle of separation of duties defined in regulations, and inform BCRA the above information.	FIs should define IT service-related roles, responsibilities, and responsibility sharing models with service providers, ensure separation of responsibilities, and inform BCRA above information. FIs can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. HUAWEI CLOUD clearly defines a security responsibility sharing model with FIs, for details on the security responsibilities of both tenants and HUAWEI CLOUD, please refer to the ***Huawei Cloud Data Security White Paper*** released by HUAWEI CLOUD. In addition, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two- factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure that user creation, authorization, and authentication to rights collection

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different responsibilities in different positions are limited to access the equipment under their role.
7.7.1	Information Security Government technical-operational requirements	RGS002: FIs/ service providers must establish roles and responsibilities for processing their customer data, and they must be formally established in the IT service agreement.	For the customer data of FIs, FIs should establish relevant data processing roles and responsibilities, and clearly establish their respective roles and responsibilities in the IT service agreements signed with service providers. As the Cloud Service Provider (CSP), HUAWEI CLOUD is responsible for the platform security defined by the security and compliance of HUAWEI CLOUD's infrastructure, including the cloud platform and software applications offered to FIs, to help FIs protect their content data. For details on the data security responsibilities of both tenants and HUAWEI CLOUD, please refer to the ***Huawei Cloud Data Security White Paper*** released by HUAWEI CLOUD.
7.7.1	Information Security Government technical-operational requirements	RGS003: FIs and provider must comply with national law and regulations related to the protection of personal data (Law 25.326-PDPL) when the service involves the collection and use of personal data, which must be reflecting in the IT service agreements.	FIs should identify laws and regulations related to the protection of personal data and evaluate their own compliance. When selecting service providers, FIs should also evaluate service providers'compliance with laws and regulations, and require service providers to comply with relevant laws and regulations on personal data protection in the agreements signed with service providers. Huawei's cloud business follows Huawei's strategy of "one country, one customer, one policy" which complies with the safety regulations of the customer's country or region and the requirements of industry supervision. It also establishes and manages a highly trusted and sustainable security guarantee system towards the aspects of organization, process, norms,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			technology, compliance, ecology and other aspects that adheres to the best practices of the industry. In an open and cooperatives manner, we will work with relevant governments, customers and industry partners to meet the challenges of cloud security and meet the security needs of customers in an all-round way. HUAWEI CLOUD has identified and analyzed PDPL regulatory requirements. For more information, please refer to the ***HUAWEI CLOUD Compliance with Argentina PDPL*.**
7.7.1	Information Security Government technical-operational requirements	RGS004: FIs/service providers should establish and record information exchange agreements with IT service agreement participants (including third parties sub concentrated), as well as guaranteed techniques and operational measures (including format, time limit, responsible party, etc.), and provide useful, timely and complete information to the parties involved and BCRA.	FIs should sign agreements with service providers, and the agreements should include detailed techniques and operational measures in order to provide useful, timely and complete information to the parties involved and BCRA. HUAWEI CLOUD provides online version of ***HUAWEI CLOUD Customer Agreement*** and ***HUAWEI CLOUD Service Level Agreement***, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. In addition, HUAWEI CLOUD has developed its own mechanism for supplier management, conducts strict security management on outsourcers and outsourced personnel, and regularly conducts audits and security assessments on suppliers .
7.7.1	Information Security Government technical-operational requirements	RGS005: If the service provider/subcontractor is involved in providing IT services which involve processing, storing or transport FIs data overseas , the FIs/service provider/ third parties involved should provide the necessary mechanism to verify that the location satisfy the legal,	FIs should determine the type of data and the location of data storage, transmission, and processing, identify whether there are cross-border data scenarios, and analyze the requirements of relevant laws and regulations, and clearly require the service provider in the contract signed to provide the mechanisms which could verify whether data storage, transmission, and processing satisfy the legal, normative and contractual provisions.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		normative and contractual provisions established in the IT service agreement.	The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZ within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the FIs is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our FIs. We will also openly and cooperatively tackle cloud security challenges standing should-to-shoulder with our FIs and partners as well as relevant governments in order to meet all the security requirements of our cloud users.
7.7.1	Information Security Government technical-operational requireme	RGS006: The IT service agreement should include the obligation not to disclose personal data and extend such obligation to subcontracted third parties.	FIs should specify the obligation of service providers not to disclose personal data in the agreements signed with service providers. As the Cloud Service Provider (CSP), HUAWEI CLOUD is responsible for the platform security defined by the security and compliance of HUAWEI

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	nts		CLOUD's infrastructure, including the cloud platform and software applications offered to FIs, to help FIs protect their content data. The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the FIs is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our FIs. We will also openly and cooperatively tackle cloud security challenges standing should-to-shoulder with our FIs and partners as well as relevant governments in order to meet all the security requirements of our cloud users. HUAWEI CLOUD has identified and analyzed PDPL regulatory requirements. For more information, please refer to the ***HUAWEI CLOUD Compliance with Argentina PDPL***.
7.7.1	Information Security Government technical-operational requirements	RGS007: FIs/ service providers must document and assign ownership of all information assets in the IT service, determining the level of operational responsibility of each party in the information lifecycle.	FIs should establish formal asset management procedures, classify their assets, and define asset owners. HUAWEI CLOUD provides FIs with a unified management interface for FIs to query and manage cloud services. Huawei Cloud **Host Security Service (HSS)** is a security manager for servers. It provides asset management functions for FIs: manages and analyzes security asset information, such as accounts,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			ports, processes, web directories, and software.

Chapter 7.7.2 of "A" 6375 requires FIs to meet the technical operational requirements of awareness and training. The relevant control requirements and HUAWEI CLOUD's responses are as follows.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.2	Awareness and Training technical-operational requirements	RCC001: The contents of the awareness and training program should be formulated and kept up-to-date at based on an analysis of incident management vulnerabilities and results, and include, but not limited to: reported, detected and known.	FIs should have a complete awareness and training management mechanism, formulate awareness and training content according to the functions and roles of the audience, and regularly analyze and update the awareness and training content. The content includes but is not limited to: • Reported/detected/known security incidents. • Prevention techniques appropriation of personal data and credentials through "social engineering", "phishing", "vishing" and other similar attacks. • Measures and techniques to protect identity authentication credentials; • Specific recommendations on security practices on the IT service support platform; • Specific techniques for developing /acquisition/manufacturing/ implementation/approval / testing of security of IT service. FIs also should provide a communication mechanism for awareness and training program to deal with related inquiries and evacuate doubts. The awareness and training program audience must cover all necessary participants required for the specific activity process. As a cloud service provider (CSP) , HUAWEI CLOUD will provide FIs with awareness and training services
7.7.2	Awareness and Training technical-operational requirements	RCC002: The contents of the awareness and training program should include: prevention techniques appropriation of personal data and credentials through "social engineering", "phishing", "vishing" and other similar attacks.	
7.7.2	Awareness and Training technical-operational requirements	RCC005: Internal staff, personnel, IT service managers of FIs/service providers, personal of third parties involved in operational tasks and clients should understand effective communication channels to deal with complaints or problems in related processes.	
7.7.2	Awareness and Training technical-operational requirement	RCC006: With regard to the awareness and training program hearing, the following criteria should be applied: • According to the role	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	s	and function of the audience in the process, develop awareness and training content. • All necessary participants must be reached in the specific activity process, including but not limited to: internal staff, staff responsible for management of IT service, service providers and clients.	and resources, including help documents, user manuals, security implementation guides, etc. For more awareness and training services and resources provided by HUAWEI CLOUD for FIs, please refer to the official website "Training Services" . In addition, the HR management framework for HUAWEI CLOUD security personnel has been established on the basis of applicable laws. The behavior of each HUAWEI CLOUD employee must comply with applicable laws, policies, and processes, as well as the Huawei Business Conduct Guidelines (BCG). HUAWEI CLOUD employees must consistently demonstrate the required knowledge, skills, and experience. HUAWEI CLOUD will conduct the awareness and training program for employees at least once a year. This training includes but is not limited to, on-the-spot speeches and online video courses, and the awareness and training content is updated regularly. HUAWEI CLOUD implements a specialized personnel management program for key positions such as O&M engineers. This program includes: On-boarding security review, On-the-job security training and enablement, On-boarding qualifications management, Off-boarding security review.
7.7.2	Awareness and Training technical-operational requirements	RCC007: FIs/service providers should analyze awareness and training program at least once a year. The analysis includes at least the following aspects: • The number and segmentation of recipients and contents of the awareness and training program. • The awareness and training program content must cover reported/detected/known security incidents.	
7.7.2	Awareness and Training technical-operational requirements	RCC008: The contents of the awareness and training program should include: measures and techniques for the protection of the identity authentication credentials.	
7.7.2	Awareness and Training technical-operational requirements	RCC0010: The contents of the awareness and training program should include: specific recommendations on security practices on the IT service support platform.	
7.7.2	Awareness and Training	RCC012: The contents of the awareness and training program should include	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	technical-operational requirements	specific techniques for developing /acquisition/manufacturing/ implementation/approval / testing of security of IT service, ensuring that internal/external staff are properly trained to reduce failures of the implementation.	
7.7.2	Awareness and Training technical-operational requirements	RCC013: FIs/service providers should provide a communication mechanism for awareness and training program to ensure: • That recipients are continuously informed. • That recipients can make inquiries and evacuate doubts.	

Chapter 7.7.3 of "A" 6375 requires FIs to meet the technical operational requirements of access control. The relevant control requirements and HUAWEI CLOUD's responses are as follows.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.3	Access Control technical-operational requirements	RCA049: FIs/service provider must guarantee that personal data are not accessed / processed / exploited by them or any of their providers for purposes other than those established in the formal agreements of the IT service, nor are they carried out without the formal and express consent of the primary responsible for the data.	As the purchaser of products or services, FIs should decide how to use products or services to store and process content data, including possible personal data involved. Therefore, FIs are responsible for the security and compliance of content data. As a cloud service provider (CSP) , HUAWEI CLOUD identifies and protects FIs' personal data. HUAWEI CLOUD's policy, processes and operations not only resulted in the formulation of privacy protection policies but also in the deployment of active privacy control measures, such as anonymization, data encryption, system and platform security protections, all helping to ensure the security of FIs' personal data. HUAWEI CLOUD is also responsible

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			for the security and compliance of the platform and infrastructure included in the cloud service, ensuring the platform and applications' security levels comply with the requirements of applicable privacy protection laws and regulations. At the same time, HUAWEI CLOUD provides FIs with a variety of privacy protection technologies and services in order to help FIs protect their privacy, such as access control, authentication, data encryption, logging and auditing functions, in order to help FIs protect their privacy according to their commercial requirements.
7.7.3	Access Control technical-operational requirements	RCA050: FIs /service providers must ensure unrestricted access to any documentation and information related to the operation process and procedures of IT services when needed.	Regarding the operation process and procedures of IT services, FIs should establish and retain relevant documents and information, and provide channels for the supervisory body to access documents and information when necessary. FIs should also provide compliance audit reports to the supervisory body to verify the effectiveness of the security control of the IT service environment. If necessary, FIs can use HUAWEI CLOUD **Identity and Access Management (IAM)** to create a temporary user account for the supervisory body, allowing the supervisory body to access documents and information related to the operation process and procedures of IT services. HUAWEI CLOUD provides **Cloud Trace Service (CTS)** for customers to collect, store, and query operation records of cloud resources. When necessary, FIs should to provide operational records of IT services to the supervisory body. In addition, HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. If necessary, FIs can apply to Huawei Cloud for a copy of the audit report

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			through official channels.
7.7.3	Access Control technical-operational requirements	RCA051: FIs must ensure that the IT service providers have passed independent assessments, external audits and certifications of international standards to implement and support the level of control of IT services provided.	When selecting service providers, FIs should check the certification and compliance reports of the service providers to assess and verify whether the IT services provided meet the requirements. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. If necessary, FIs can apply to Huawei Cloud for a copy of the audit report through official channels. HUAWEI CLOUD follows international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.
7.7.3	Access Control technical-operational requirements	RCA052: FIs/service providers should isolate incompatible roles and implement a unified identity management strategy, including but not limited to the following: • Data encryption mechanism and communication channels; • Privileged users of the operating/application platform; • Emergency/temporary users; • Common users. FIs/service providers must also ensure that a life	FIs should establish user access management mechanisms, restrict and supervise access rights based on the principle of least privilege, identify incompatible roles, and ensure separation of duties. FIs should do a good job of data classification, and conduct risk analysis, and then, based on the risk analysis results, clarify whether the data is encrypted and the encryption measures. FIs should also establish a key management mechanism so that the confidentiality and integrity of FI data will not be compromised. Key management measures include: regularly rotating keys, formulating detailed policies and procedures to manage key life cycles and key backups. HUAWEI CLOUD provides **Identity**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		cycle of the key, key parameters, rules, algorithms, and software involved must be updated and deeply communicated to the parties.	**and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to perform role- based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. HUAWEI CLOUD implements role-based access control (RBAC) for O&M personnel. They can perform operations within authorization only. Administrative accounts and emergency accounts are granted to O&M personnel based on their responsibilities only. All applications for administrative or emergency accounts shall be reviewed and approved through multiple levels. FIs can encrypt data through HUAWEI CLOUD's data storage and encryption service. HUAWEI CLOUD encapsulates complex data encryption and decryption, and key management logic, which makes the operation of customer's data encryption easy. At present, cloud hard disk, object storage, mirror service and relational database, and other services provide data encryption (service-side encryption) function using high-intensity algorithms to encrypt stored data. For data in transmission, when customers provide Web site services through the Internet, they can use certificate management services provided by the HUAWEI CLOUD United Global Well- known Certificate Service Provider. By applying for and configuring certificates for Web sites, the trusted identity authentication of Web sites and secure transmission based on encryption protocols are realized. In view of the scenario of hybrid cloud deployment and global layout of customer services, we can use the **Virtual Private Network**

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(VPN),**Direct Connect (DC)**, **Cloud Connect (CC)**, and other services provided by HUAWEI CLOUD to realize business interconnection and data transmission security between different regions. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full- lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, FIs' master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. Even Huawei O&M personnel cannot obtain the root key. DEW also allows FIs to import their own keys as master keys for unified management, facilitating seamless integration with customers' services. In addition, HUAWEI CLOUD O&M accounts are centrally managed on the LDAP platform and automatically audited. This ensures that the entire process, including user creation, authorization, authentication, and permission reclaiming, is manageable. RBAC is implemented based on service dimensions and service responsibilities. O&M personnel can access devices within their authorization only.

Chapter 7.7.4 of "A" 6375 requires FIs to meet the technical operational requirements of Integrity and Registration. The relevant control requirements and HUAWEI CLOUD's responses are as follows.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.4	Integrity and Registration technical-operational requirements	RIR003: IT services provided by service providers should record all activities and be traceable, and be able to identify "who (account, origin, destination), what (activity, function, transaction), and where (service, location), When (time) and how (pattern, ratio of events).".	FIs should record all activities and operations, the contents of the records include but are not limited to: • User ID; • Date, time and details of key events, such as login and logout; • Equipment identification or location (if possible), and system identification; • Network address and protocol; • System successful and failed login attempts; • System data, file and resource access operations; • System configuration modification; • Use of privileged accounts. FIs should also establish a lifecycle management mechanism for log data to ensure that all activities can be traced back. The retention period of logs should also meet regulatory requirements. At the same time, FIs should also formulate a forensic investigation management mechanism to prevent tampering of log data during the legal protection period, to support forensic investigations of security incidents. **HUAWEI CLOUD Trace Service (CTS)** provides operating records of cloud service resources for users to query, and for auditing. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within Huawei's cloud system. CTS inspects the log data sent by various services to ensure that the data itself does not contain sensitive information in the following; In the transmission phase, it ensures the accuracy and comprehensiveness of log information transmission and preservation by means of identity authentication, format checking, whitelist checking and a one-way receiver system; In the storage phase,
7.7.4	Integrity and Registration technical-operational requirements	RIR023: Require financial institutions/service providers to establish a life cycle management mechanism for log data, to ensure that all activities can be traced, and to comply with laws and security regulations for log storage, and unchanged by the legal time of conservation and their accessibility to those responsible for control to support forensic investigations in cases of security incidents and detection of the security breach.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			it adopts multiple backups according to Huawei's network security specifications and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. Additionally, HUAWEI CLOUD manages behavioral logs for all physical devices, networks, platforms, applications, databases, and security systems, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. HUAWEI CLOUD has established a forensic investigation management mechanism in accordance with legal requirements and formulated a standardized forensic process to support forensic investigations of security incidents.
7.7.4	Integrity and Registration technical-operational requirements	RIR010: The devices/equipment and/or pieces of software arranged by the provider for the IT service, must ensure that they satisfy the development life cycle requirements, based on the following conceptual stages: • Analysis of the requirements; • Acquisition/development; • Testing and approval; • Implementation; • Operation and maintenance; • Discard and replace . This cycle must also provide security elements related to, but not limited to, the following:	FIs should clearly specify in the service agreement the quality and security requirements that the equipment and/or software provided by the service provider must meet, and the FIs should be responsible for managing the security of the entire life cycle of the devices/equipment and/or pieces of software it owns. Huawei development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. HUAWEI CLOUD strictly complies with the security coding specifications of various programming languages issued by Huawei. Static code analysis tools are used for routine checks, and the resulting data is entered in the cloud service tool chain to evaluate the quality of coding. Before all cloud services are released, static code analysis alarms must be cleared to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		• Functional security requirements; • Types and characteristics of validation of input data; • Granularity of functions and records; • Access levels; • Control changes; • Update and patches.	effectively reduce the security issues related to coding when online. To meet FIs compliance requirements, HUAWEI CLOUD has also developed change management procedures to application and infrastructure changes. After the change application is generated, the change manager shall make a change level judgment and submit it to the HUAWEI CLOUD change committee, which shall pass the review before implementing the change as planned. All changes are fully validated prior to application through class production, bad condition testing, gray release, Blue Green Deployment, etc. to ensure that the change committee has a clear understanding of the change action, duration, fallback action of the change failure, and all possible impacts.
7.7.4	Integrity and Registration technical-operational requirements	RIR011: FIs/providers must execute a process of approval of devices /equipment and/or pieces of software to interact with the IT service, ensuring the verification of all aspects of design, functionality, interoperability and safety features defined in the procurement/manufacturing/development and deployment stages.	
7.7.4	Integrity and Registration technical-operational requirements	RIR020: FIs/ service providers must have preventive and corrective mechanisms in order to respond to personal data subjects' requests for access, modification and deletion of their personal data when protecting the rights of personal data subjects.	FIs should decide how to use products or services to store and process content data, including personal data that may be involved, and FIs are responsible for content data security and compliance. FIs should also correctly and comprehensively identify personal data in the cloud, formulate strategies to protect the security and privacy of personal data, and choose appropriate privacy protection measures to protect the rights of personal data subjects. As the Cloud Service Provider (CSP), HUAWEI CLOUD is responsible for the platform security defined by the security and compliance of HUAWEI CLOUD's infrastructure, including the cloud platform and software applications offered to FIs, to help FIs protect their content data. The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			and industry supervision requirements of the country or region where the FIs is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our FIs. We will also openly and cooperatively tackle cloud security challenges standing shoulder-to-shoulder with our FIs and partners as well as relevant governments in order to meet all the security requirements of our cloud users. HUAWEI CLOUD has identified and analyzed PDPL regulatory requirements. For more information, please refer to the ***HUAWEI CLOUD Compliance with Argentina PDPL***.
7.7.4	Integrity and Registration technical-operational requirements	RIR021:FI/providers should ensure and establish mechanisms for recovering information assets in the event of termination and/or indefinite interruption and/or relocation of services, respecting the conditions of information security and continuity of operations.	FIs should establish their own business continuity mechanisms and formulate RTO and RPO indicators to ensure their key businesses. If FIs need HUAWEI CLOUD's participation in the process of running their internal business continuity plans, HUAWEI CLOUD will actively cooperate. FIs rely on the multi-region and multi-available area (AZ) architecture of HUAWEI CLOUD data center cluster to achieve the flexibility and availability of their business systems. Data centers are deployed around the world, so FIs will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			transfers FIs applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected FIs. HUAWEI CLOUD also deploys a global load-balanced management center, where the FIs' applications enable N+1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. FIs can use HUAWEI CLOUD's data backup and archive service to minimize data loss in the event of a disaster. HUAWEI CLOUD has a comprehensive disaster recovery plan that regularly undergoes tests. HUAWEI CLOUD ensures that cloud services are running in the event of a disaster. In addition, as a cloud service provider (CSP) , HUAWEI CLOUD provides FIs with cloud services that their business depends on. Therefore, except for outsourcing interruptions or unexpected terminations caused by force majeure, HUAWEI CLOUD formulates business continuity management systems for the cloud to suit the FIs' business needs, provides continuous and effective services for FIs to ensure the business development of FIs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response.
7.7.4	Integrity and Registration technical-operational requirements	RIR022: The resources and information used in the IT service must be inventoried with their current identification of the owner and indicating the deletion parameters safe storage and their validation parameters in the data lifecycle.	FIs should conduct unified management of their information assets, define the owners of information assets, and establish security control measures for the entire life cycle of data, including data storage and deletion. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full- lifecycle key

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			management. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, FIs' master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. Even Huawei O&M personnel cannot obtain the root key. DEW also allows FIs to import their own keys as master keys for unified management, facilitating seamless integration with FIs' services. Regarding data isolation, HUAWEI CLOUD recommends that data be distinguished and isolated at the beginning of the data life cycle by running a classification and risk analysis on the client's data. Based on the risk analysis results, clarify the storage location, storage services and security measures to protect data. When FIs use cloud hard drive, object storage, cloud database, container engine and other services, HUAWEI CLOUD ensures that FIs can only access their own data through different granularity access control mechanisms such as volume, bucket, database instance, container and so on. When FIs take the initiative to delete data or delete data due to the expiration of service, HUAWEI CLOUD will strictly follow the data destruction standard and the agreement with FIs to remove stored FIs data. For more information on data deletion, please refer to the *White Paper for HUAWEI CLOUD Data Security*.
7.7.4	Integrity and Registratio	RIR024: FIs/service providers are required to establish two data	FIs should determine how to configure the environment and protect their data, including whether to encrypt data

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
	n technical-operational requirements	encryption strategies, storage encryption and transmission encryption.	(storage encryption and transmission encryption), and determine the security functions/tools used. FIs can encrypt data through HUAWEI CLOUD's data storage and encryption service. HUAWEI CLOUD encapsulates complex data encryption and decryption, and key management logic, which makes the operation of FIs' data encryption easy. Currently, services including Elastic Volume Service (EVS), Object Storage Service (OBS), Image Management Service (IMS) and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. The encryption function of the server integrates the key management function (DEW) of Huawei's cloud data encryption service. For data in transmission, when FIs provide Web site services through the Internet, they can use certificate management services provided by the HUAWEI CLOUD United Global Well-known Certificate Service Provider. By applying for and configuring certificates for Web sites, the trusted identity authentication of Web sites and secure transmission based on encryption protocols are realized. In view of the scenario of hybrid cloud deployment and global layout of FIs services, we can use the **Virtual Private Network (VPN)**, **Direct Connect (DC)**, **Cloud Connect (CC)**, and other services provided by HUAWEI CLOUD to realize business interconnection and data transmission security between different regions. HUAWEI CLOUD provides **Data Encryption Workshop (DEW)** for FIs. The key management function in DEW can centralize key management throughout the life cycle. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			association configuration on DEW Console or using APIs, FIs' master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. Even Huawei O&M personnel cannot obtain the root key. DEW also allows FIs to import their own keys as master keys for unified management, facilitating seamless integration with FIs' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys.
7.7.4	Integrity and Registration technical-operational requirements	RIR025: FIs should ensure that they are logically separated from other third-party organizations in the processing, storage, transmission and recovery of data. If necessary, if a service provider wants to access the equipment/software of FIs, it must obtain the permission of FIs and obtain the relevant authorization in advance.	It is recommended that FIs distinguish and isolate data at the beginning of the data life cycle. FIs first classify data and conduct risk analysis, and then, based on the results of risk analysis, clarify the storage location, storage services, and security protection measures of the protected data. When FIs use cloud hard drive, object storage, cloud database, container engine and other services, HUAWEI CLOUD ensures that FIs can only access their own data through different granularity access control mechanisms such as volume, bucket, database instance, container and so on. In the scenario of FIs self-built storage, for example, when installing database software on virtual machine instances, it is suggested that FIs use **HUAWEI CLOUD's Virtual Private Cloud (VPC)** service to construct a private network environment, divide the network area through subnet planning, routing policy configuration, place the storage in the internal subnet, and configure the network ACL and security group rules to access the subnet, as well as strictly controlling

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			the network traffic of the virtual machine. HUAWEI CLOUD will not access the cloud environment of financial institutions, except during maintenance, HUAWEI CLOUD will only log in to the FIs' console or resource instance to assist the FIs in maintenance after it has been authorized by the FIs (i.e. providing account/password).

Section 7.7.5 of "A" 6375 requires FIs to meet the technical operation requirements for control and monitoring. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.5	Control and Monitering technical-operation requirements	RMC003: FIs/service providers should track changes in their ITS to ensure configuration and verify update levels of operating systems, databases, communication links, malicious code detection and prevention tools, network security equipment, drivers, and any other security tools. They should include, but should not be limited to: • Tracking privileges and access rights; • Information copying, safeguarding and recovery processes; • Availability of devices/ equipment; • Alarms, alerts and problems detected by the event registration systems.	FIs should be responsible for defining their operational models and establishing change management processes. The tools provided by the service provider can be used to detect and track changes in their environment and resources, to evaluate and review changes to their environment and resource allocation. FIs pass through HUAWEI CLOUD's **Cloud Eye Service (CES)** which provides three-dimensional monitoring of **Elastic Cloud Server (ECS)**, bandwidth, and other resources. The monitoring object of CES is the resource usage data of infrastructure, platform, and application services and does not monitor or access tenant data. CES can currently monitor multiple indicators of cloud services, these metrics allow users to set alert rules and notification policies to keep abreast of the health and performance of instance resources for each service. FIs can scan for external vulnerabilities and operating system vulnerabilities. They can detect asset content compliance, scan the configuration to compare it against the baseline, detect weak passwords, and perform other such functions
7.7.5	Control and Monitering technical-operation requirements	RMC004: FIs should have transactional monitoring mechanisms to monitor suspicious incidents or threats, such as installing systems to monitor and	

		analyze cyber threats so that FIs can detect, prevent and deal with suspicious incidents or threats in a timely manner: • Preventive. Detecting, triggering communication actions with the client by alternative means before confirming operations. • Reactive. Detecting and firing communication actions with the client in a post-confirmation of suspicious operations. • Assumed. Detecting and assuming the return of the sums involved or the customer's claims for misrecognition of transactions made.	through HUAWEI CLOUD **Vulnerability Scan Service (VSS).** It can automatically discover the security risks of websites or servers exposed in the network, and help users to secure their business on the cloud from multiple dimensions. HUAWEI CLOUD **Image Management Service (IMS)** provides simple and convenient self-service management functions for images. Tenants can manage their images through the IMS API or the management console. HUAWEI CLOUD staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. In addition, in order to ensure the security and stable operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness.
7.7.5	Control and Monitering technical-operation requirements	RMC006: Based on the logs collected by the ITS resources associated with the scenario, FIs/service providers must perform a classification and determination of events, a definition of commitment limits and thresholds, normal/unexpected behavior levels, and establish actions in accordance with each classification and determined limits.	FIs should ensure the operation of the system and network problem get timely and effective solution, ensure that there is a formal record of the event management process, the process should be clearly recorded in event management process (including the issue and event records, analysis, repair, and monitoring) of employees' roles and responsibilities, the time limits of events escalation and events solution, to record and track details of events, analyze the cause of the events and find out the root cause to prevent the events from happening again. **Cloud Eye Service (CES)**provides FIs with a robust monitoring platform for Elastic **Cloud Server (ECS)**,

			bandwidth, and other resources. CES monitors alarms, notifications, and custom reports and diagrams in real time, giving the user a precise understanding of the status of service resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service. At the same time, HUAWEI CLOUD can also provide an Anti-DDoS, Web Application Firewall (WAF), **Database Security Service (DBSS)**, and **Cloud Trace Service (CTS)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application-level and data-level attacks, as well as reviewing and auditing incidents. In addition, HUAWEI CLOUD, as a CSP, is responsible for the event and change management of its infrastructure and various cloud services such as IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a complete event and management process to regularly review and update it. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source. HUAWEI CLOUD has also formulated information security event management specifications, which stipulate the classification and escalation rules of security events, as well as the response time and resolution time limits for events of different levels.
7.7.	Control and	RMC014: FIs/service	For IT services provided by service

5	Monitering technical-operation requirements	providers should determine, document and proceed with the resources, devices/equipment and pieces of software to monitor the activities of the IT service.	providers, FIs should be responsible for defining the operation model of IT services, monitoring and managing the IT service activities. FIs can monitor the use and performance of their own cloud resources through HUAWEI CLOUD monitoring services **Cloud Eye Service (CES)**. HUAWEI CLOUD can also provide service reports according to SLA and FIs needs. If FIs need to conduct inspection and due diligence on HUAWEI CLOUD and its operation, HUAWEI CLOUD will organize a dedicated person to assist. Cloud Eye Service provides users with a robust monitoring platform for flexible cloud servers, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to detect anomalies of cloud resources in time and take countermeasures. In addition, in order to ensure the security and stable operation of Huawei's cloud platform and network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles, and testing of backup effectiveness.
7.7.5	Control and Monitering technical-operation requirements	RMC015: FIs/service providers should formally establish and periodically run vulnerability analysis and result analysis in all the critical businesses.	FIs should perform vulnerability scans and fixes on a regular basis for critical businesses and analyze the results. HUAWEI CLOUD provides **Vulnerability Scan Service (VSS)** for FIs to scan for vulnerabilities on their websites, operating systems, asset compliance, and baseline configuration and weak passwords. VSS automatically discovers security risks of websites and servers to secure

			FIs' business on the cloud from multiple dimensions. In addition, HUAWEI CLOUD manages vulnerabilities based on its vulnerability management system to ensure that vulnerabilities on self-developed and third-party infrastructure, platforms, application layers, cloud services, and O&M tools are detected and fixed within the time specified in SLA. This reduces risks caused by malicious exploitation of vulnerabilities and adverse impacts on FIs businesses. For vulnerabilities that involve the cloud platform and FIs businesses, HUAWEI CLOUD will push the vulnerability mitigation and recovery suggestions and solutions to end users and FIs in a timely manner after making sure that no high attack risks will be caused by proactive disclosure. HUAWEI CLOUD will face the challenges brought by the security vulnerabilities together with FIs.

Section 7.7.6 of "A" 6375 requires FIs to meet the technical operation requirements for incident management. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.6	Incident Management technical-operation requirements	RGI001: FIs/service providers should implement risk analysis and security incident analysis at least once a year, and according to the results of the analysis, develop protective measures, security awareness and skills training, log management mechanism, incident monitoring and warning mechanism, etc.	FIs should ensure the operation of the system and network problem get timely and effective solution, ensure that there is a formal record of the event management process, the process should be clearly recorded in event management process (including the issue and event records, analysis, repair, and monitoring) of employees' roles and responsibilities, the time limits of events escalation and events solution, to record and track details of events, analyze the cause of the events and find out the root cause to prevent the events from happening again. FIs should also ensure that the appropriate personnel can be contacted in the event of a security incident and take immediate measures in the event of a
7.7.6	Incident Management technical-operation requirements	RGI002: It is required to establish event warning signs according to statistical information such as event	

		type/frequency/mode, and provide security suggestions.	security incident. To cooperate with FIs to meet compliance requirement, to ensure the professionalism and urgency of security event handling, HUAWEI CLOUD has a 24/7 professional security event response team, and a corresponding security expert resource pool.HUAWEI CLOUD formulates the classification and escalation principle of information security incidents, ranking them according to their degree of impact on the FIs' business, and initiates a process to notify FIs of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple FIs, HUAWEI CLOUD can promptly notify FIs of events with an announcement. The contents of the notification include but are not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for FIs. After the incident is resolved, the incident report will be provided to FIs according to the specific situation. In addition, HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. HUAWEI CLOUD annually tests information security incident management procedures. All of information
7.7.6	Incident Management technical-operation requirements	RGI003: Security incident management can be executed in an outsourced manner but should be coordinated with FIs staff.	
7.7.6	Incident Management technical-operation requirements	RGI005: Incidents detected should be treated regularly with escalation formally defined.	

			security incident response personnel, including reserve personnel, need to participate. The test scenarios are combined with the current common network security threats, in which high-risk scenarios will be tested during simulations. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After their completion, relevant personnel will redact a report and summarize any problems identified during the simulation. If the results are indicating issues with the information security incident management and process, related documentation will be accordingly updated. HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes.

Section 7.7.7 of "A" 6375 requires FIs to meet the technical operation requirements for minimum operational continuity. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.7.7	Minimum Operational Continuity technical-operation requirements	RCO001: The necessary resources are required to create, maintain, update, and test data processing continuity plans. The plan must be operational based on the requirements agreed with the service provider, the requirements of the FIs themselves and regulated by the BCRA.	FIs should require service providers to develop business continuity plans, for critical or broad impact activities, and to allocate adequate resources for such activities in accordance with the FIs own business continuity and regulatory requirements. FIs should also regularly test business continuity plans with key service providers, and the results must be documented. FIs can rely on HUAWEI CLOUD data center cluster multi-region (Region) and multi-available zones (AZ) architecture to implement disaster tolerance and backup of their business systems. Data centers are
7.7.7	Minimum Operational Continuity technical-operation	RCO002: FIs/service providers should define, document and implement risk assessment, to determine the impact of an	

	requirements	event (events may disrupt the activities of the organization of FIs, service providers or third parties subcontracted), including but not limited to: • Identification of critical resources, including operational and control users; • Identification of all dependencies, including application processes, peers, and subcontracted third parties; • Detection of threats from critical resources; • Determination of the impact of planned outages or not, and their variation in time; • Establishment of a maximum tolerable period of interruption; • Establishment of partial and total recovery periods; • Establishment of the maximum tolerable interrupt time for recovery critical resources; • Estimation of the resources required for continuity and eventual restoration of operation and alternative locations. In addition, people responsible for primary processes and critical resources should also be actively involved to ensuring full coverage of ITS partners.	deployed around the world, so FIs will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers FIs applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected FIs. HUAWEI CLOUD also deploys a global load-balanced management center, where the FIs' applications enable N+1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure. In addition to providing high-availability infrastructure, redundant data backup centers, and disaster preparedness in available areas, HUAWEI CLOUD has also developed business continuity plans and disaster recovery plans that are regularly tested to ensure that the emergency plan is in line with the current organizational and IT environment. FIs can use HUAWEI CLOUD's data backup and archive service to minimize data loss in the event of a disaster. HUAWEI CLOUD has a comprehensive disaster recovery plan that regularly undergoes tests. HUAWEI CLOUD ensures that cloud services are running in the event of a disaster. In addition, HUAWEI CLOUD, as a cloud service provider, provides FIs with cloud services on which their business depends. Therefore, HUAWEI CLOUD has established a business continuity management system in line with its own business characteristics, providing services for financial institutions continuously and effectively, and ensuring the development of financial institutions' business. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year and conducts emergency drills and tests regularly to continuously optimize emergency response.
7.7.7	Minimum Operational Continuity technical-operation	RCO003: The data processing continuity plan should consider, but not be limited to, incorporation of the following contents:	

	requirements	• Manual, logistical and automated emergency operating procedures according to each identified process/resource and particular action; • Location/location, transfer and transport of managers, suppliers and services emergency resources and physical and logical resources; • Procedures for recovering/restoring committed resources.	
7.7.7	Minimum Operational Continuity technical-operation requirements	RCO004: The data processing continuity plan should be tested periodically, at least once a year. The tests must be consistent and consistent with the criteria of the RCO002 requirement. The tests must also ensure that all those responsible and participants in the continuity and recovery processes are regularly, continuously and formally informed.	

6 How HUAWEI CLOUD Meets the Requirements of BCRA “A”7266

"A" 7266 is directed primarily to financial institutions, payment service providers that offer payment accounts, and financial market infrastructures. The guidelines include a range of effective cyber incident response and recovery practices, which are dedicated to improving cyber resilience across the financial ecosystem.

When FIs are seeking to comply with the requirements provided in the "A" 7266, 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 "A" 7266, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

6.1 Government

Section 2.1 of "A" 7266 defines the governance framework for cyber incident response and recovery. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.1.1	Culture	It is expected that the management of the entity will accompany the creation of an organizational environment where it promotes reporting or escalating cyber incidents through a channel established for this purpose, considering: 2.1.1.1 The establishment of training programs for all levels of the entity, which promote proactive behaviors, where the possibility of occurrence of cyber incidents and learning based on errors is accepted. 2.1.1.2 Promote a positive	FIs should establish their own mechanisms for business continuity and develop RTO and RPO metrics to ensure the continuity of their key businesses. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate. FIs should establish an information security incident management mechanism and specify the roles and responsibilities in the incident management process. HUAWEI CLOUD has developed a complete mechanism for internal

		culture towards cyber incident management, ensuring that this information is used as a source to improve the preparedness stage. 2.1.1.3 Promote continuous and sustained actions with suppliers and third parties in the preparation of response and recovery tasks to cyber incidents, so that they can be timely and adapted to different situations.	security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, HUAWEI CLOUD will provide the incident report to the customer according to the specific situation.
2.1.2	Organization, roles, functions and responsibilities	2.1.2.1 The governance of response and recovery activities is part of the overall governance of the organization. The objectives and priorities of these guidelines would have to be aligned with the management of the general risk of the organization, in the same way the roles and responsibilities and the processes necessary to facilitate decision making have to be defined. 2.1.2.2 The management of the organization is responsible for the definition of the objectives cyber resilience, as well as implementing related policies, procedures and controls. 2.1.2.3 For coordination and communication actions in the face of a cyber incident, it is advisable to define a role of "coordinator," which can be a person or group. Depending on the criticality, the "coordinator" must have the ability to take decisions during the cyber incident, to initiate certain activities and contact those involved. 2.1.2.4 Cyber incident response and recovery activities help ensure the security and reliability of financial services. The management of the entity can promote these activities not only by providing its support, but also by allocating the	

		necessary budget for the acquisition of technological tools or the implementation of awareness, training and communication programs at all levels of the organization, among others.	
2.1.3	Reports, metrics and accountability of activities	Effective management is achieved by establishing metrics to assess the impact of cyber incidents, to measure the efficiency of response and recovery activities, and to prepare corresponding reports to authorities. Depending on the criticality and/or priority of the incident, the urgency of attention and the appropriate level of escalation will be defined, given that for example a highly critical cyber incident will most likely require to be informed to the management of the entity.	

6.2 Planning and Preparation

Section 2.2 of "A" 7266 provides specific measures to establish and maintain the capability of organizations to respond to cyber incidents. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.2.2	Strategy, channels and communication plans	2.2.2.1 Contact lists of all potential stakeholders should be established, both internal and external, which should be reported depending on the scenarios and criteria identified. 2.2.2.2 It is advisable to establish communication strategies with the participants and each of the identified audiences. Plans may include models of possible content to be reported according to the type of cyber-incidents taking into account the appropriate or	FIs should prepare their stakeholders and its contact information. FIs should also formulate incident communication policy to clarify communication channels and report content templates after the occurrence of incidents. HUAWEI CLOUD regularly conducts risk assessment according to the requirements of the internal business continuity management system, identified and analyses the potential risks faced by key resources supporting the continuous operation of cloud services. HUAWEI CLOUD further considers

		available communication channel. It is considered desirable to assess the sequence of information to be published during an incident taking into account the audience with which it is shared and the need to keep those involved informed in order to reduce uncertainty and increase confidence.	emergency scenarios and risks, and formulates crisis management procedures to deal with and minimize the impact of various emergencies. Crisis management procedures include early warning and reporting of emergencies, emergency escalation, the conditions for starting emergency plans, notification of event progress, and internal and external communication processes.
2.2.3	Incident assessment scenarios and criteria	2.2.3.1 Plans and procedures should include the criticality of possible scenarios based on low-probability and high-impact events backed by threat intelligence. These scenarios may: i) be assessed during the Business Continuity Plan or the response and recovery plan tests, and ii) be tested internally, with external parties, with relevant authorities, service providers or third parties, where applicable. 2.2.3.2 The effectiveness of IRRC activities can be assessed during a test and in the face of actual incidents. The participation of independent observers is recommended to maintain an objective assessment and obtain accurate records of each step, as well as the documentation of actions and decision making during and after a cyber incident.	Customers should establish a situational awareness management mechanism to ensure that the information and information processing facilities in the network are protected. The HUAWEI Product Security Incident Response Team (PSIRT) became an official member of the Forum of Incident Response and Security Teams (FIRST) in 2010, through which HUAWEI PSIRT and the other 471 members can share incident response best practices and other security information. HUAWEI PSIRT has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD's self-service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on inhouse-developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations. In addition, HUAWEI PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification response, and disclosure. HUAWEI CLOUD manages vulnerabilities based on its vulnerability management system to ensure that vulnerabilities on self-developed and third-party infrastructure, platforms, application layers, cloud services, and O&M

			tools are detected and fixed within the time specified in SLA. This reduces risks caused by malicious exploitation of vulnerabilities and adverse impacts on customers businesses. See section 8.2 Vulnerability Management of HUAWEI CLOUD Security White Paper for more information.
2.2.4	Infrastructure for recovery	Depending on the size, complexity and risk of the entity, it may be necessary to monitor 24x7 or use third party security services to achieve the objective of identifying, detecting, responding and investigating cyber incidents that may affect infrastructure, services and/or customers.	Customers should manage and monitor the cloud services they use to ensure that suppliers can provide sufficient resources and services according to relevant requirements. Cloud Eye Service (CES) provides users with a robust monitoring platform for Elastic Cloud Server (ECS), bandwidth, and other resources. CES provides real-time monitoring alarms, notification and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.
2.2.5	Disaster Recovery and Resilience Infrastructure	Resilience is built through the use of diversified infrastructure and replication of critical systems, disaster recovery sites, or alternative sites with different geographic risk profiles. This requires identifying the risk in external third parties, assessing and adopting mitigation techniques when available.	FIs can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.
2.2.6	Capabilities and records for	The development of proper log management includes tools to collect and store system logs that will be necessary for the investigation and analysis of	FIs should develop a monitoring mechanism regarding sensitive data, networks, systems, databases and security modules. In order to cooperate with customers to meet

	research	incidents. The types of logs that are collected and the retention period should be defined in advance, based on the classification of the information, of the rules and regulations in force. Technical and forensic capabilities are necessary to preserve evidence and analyze control failures, identify security issues and other causes related to a cyber incident. If you do not have your own capabilities, you can hire a third-party service. Forensic personnel need to be adequately trained and follow standardized procedures to preserve the integrity of evidence, data and systems during investigations.	regulatory requirements, as a cloud service provider, HUAWEI CLOUD's Cloud Trace Service (CTS) provides operating records of cloud service resources for users to query, for auditing and backtrack use. There are three types of operations recorded: operations performed through the cloud account login management console, operations performed through APIs supported by cloud services, and operations triggered within HUAWEI's cloud system. CTS inspects the log data sent by various services that ensures the data itself does not contain sensitive information. In the transmission phase, it guarantees the accuracy and comprehensiveness of log information transmission and preservation by means of identity authentication, format checking, whitelist checking and a one-way receiver system; In the storage phase, it adopts multiple backups according to HUAWEI's network security specification and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance.
2.2.7	Service Providers	In order to ensure an adequate response during cyber-incidents, it is considered necessary to have a detail of the services contracted to third parties, the providers of those services, and the key details of	FIs should ensure that their selected service providers can provide services in accordance with the contract and SLA. HUAWEI CLOUD provides online version of HUAWEI CLOUD Customer Agreement and HUAWEI

		the agreements such as the contact information of the service provider, the validity period and agreed service levels. Subcontractors' service agreements must also be reviewed. In relation to the complexity and size of the service, the cyber incidents of the providers can be assessed, especially the risks of their cybersecurity practices in data storage in third parties and/or security vulnerabilities of "software" in supply chain management or supplier systems.	CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. Currently, HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications and is audited by third parties every year. If necessary, FIs can apply to HUAWEI CLOUD for a copy of the audit report through official channels. To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services. According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity, etc. If a customer applies, HUAWEI CLOUD will provide the customer with a copy of the relevant information security management system as needed.

6.3 Analysis

Section 2.3 of "A" 7266 deals with forensic analysis, determining criticality and impact of cyber incidents, and investigating root causes. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.3.1	Cyber Incident Taxonomy	2.3.1.1 A predefined taxonomy is required to classify cyber-incidents according to parameters such as: type of incident, threat actors, threat vectors and their impacts, and a pre-established evaluation framework to prioritize incident response based on criticality of systems or services. 2.3.1.2 Having pre-established analysis of cyber incidents helps to prioritize timely attention and allocate resources to mitigate impact, restore services and recover, at the same time, allows information to be communicated in simple language. Criticality levels are set to give an immediate response, as the first few hours after an incident are often the most critical to containment. Also, this approach allows a first attention without knowing the incident completely.	FIs shall establish a classification standard for information security incidents and prioritize incidents handling according to this standard. HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly

			notify customers of events with an announcement. The contents of the notification include but not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, HUAWEI CLOUD will provide the incident report to the customer according to the specific situation.
2.3.2	Forensic research and analysis	2.3.2.1 For the forensic investigation of the incident, it is necessary to have "logs" or audit logs of the systems and devices. Analyzing alerts, indicators (security and systems), investigating and correlating events will enable the response team to determine the impact of an incident and possibly identify the source. For the answer, data are also retrieved from the computer devices involved in the interaction such as those connected to the network, processes in execution, user sessions, open files, from the relevant equipment their configurations and memory contents, among others. The integrity of such data must be ensured for proper analysis. 2.3.2.2 At the time of a forensic investigation it will be important that the systems from which the system records are obtained are synchronized. 2.3.2.3 It is recommended to have a variety of internal and external sources of information for a rapid assessment of threats and the causes of a cyber incident.	Customers should formulate the cloud forensics process and control measures according to their risk preferences to ensure the confidentiality, integrity and availability of data during cloud forensics. HUAWEI CLOUD strictly adheres to "not accessing customer data without permission" and explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. In addition, the server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD Data Encryption Workshop (DEW), which provides full-lifecycle key management. Without authorization, no one except the customer can obtain keys to decrypt data, which ensures the confidentiality, integrity and availability of the data in the process of cloud forensics. In addition, HUAWEI CLOUD's Cloud Trace Service (CTS) provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location.

6.4 Mitigation

Section 2.4 of "A" 7266 provides mitigation measures to reduce the impact of cyber incidents on operations and services. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.4.1	Containment, isolation and eradication	2.4.1.1 Containment measures are deployed according to the type of cyber incident to prevent it from causing further damage both within a target subject and to the others with which it is connected or related. Having information on current cyber threats, in the form of engagement indicators and analyzing potential impacts also contributes to the definition of containment measures, in monitoring network activity and for decision making. In the event of an incident, insurance coverage may be helpful in recovery. 2.4.1.2 In the event of serious incidents, in order to make the decision to shut down, disconnect or isolate part of the systems or networks as a mitigation measure or to continue providing service, the costs, the impact on the "Business" and operational risks, among others, must be considered. 2.4.1.3 After the collection of evidence and its preservation, all elements that had been introduced by the attackers must be removed, such as malicious code and data, among others. In addition, the configurations or alterations to the systems that have been affected will have to be corrected. Activities to eradicate the incident could include tasks such as patching and checking vulnerabilities, among others.	FIs should develop a network security risk assessment mechanism to analyze the potential impact and determine preventive measures based on the collected network threat information. After the occurrence of a major incident, should promptly respond to and remedy related vulnerabilities. FIs should conduct risk assessments on the use of HUAWEI CLOUD services in accordance with their risk preferences, the results of the risk assessment should be documented, and the mechanisms (such as evaluation cycles) for monitoring and managing HUAWEI CLOUD services should be determined based on the results of the risk assessment. HUAWEI CLOUD will cooperate with customers in risk assessment work as needed.

2.4.2	Measures for "Business Continuity"	Depending on the criticality of the cyber incident and according to its consequences or impact, the Business Continuity Plan could be activated.	FIs should establish their own mechanisms for business continuity and develop RTO and RPO metrics to ensure the continuity of their key businesses. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate. To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business

			continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.

6.5 Restoration and Recovery

Section 2.5 of "A" 7266 specifies the activities to restore the affected business and services to the normal state in a secure manner. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.5.1	Prioritization	The prioritization of recovery activities has to be done according to the criticality of the business processes, in order to recover the data and the systems that support them. The importance of having an updated list of internal and external contacts is highlighted.	FIs should develop incident recovery mechanism. Prioritize business recovery based on the results of business Impact analysis (BIA), and maintain internal and external contact lists and contact information. During the incident recovery process, FIs should monitor the recovery process. After recovery is complete, its IT assets should be tested to ensure that their integrity has not been compromised. HUAWEI CLOUD has set up a dedicated team to support and communicate with customers. Customers can seek help from HUAWEI CLOUD through the worksheet service.
2.5.2	Data recovery	2.5.2.1 In order to comply with the business requirements in data recovery, it is necessary to have the necessary information in both its own and third-party locations and, in this sense, when a cyber incident occurred, the integrity of the data must be guaranteed, that is, that have not been tampered with or corrupted before restoration. To ensure data integrity, availability and readability, restoration tests are also required on a regular basis. 2.5.2.2 It is desirable that restoration activities have automated, documented and tested procedures, thus reducing the risk of human	

		error that can arise in a manual restoration. Uncompromising images and snapshots of the system are often used to restore affected systems and must be regularly reviewed, tested and stored securely to mitigate damage or destruction. 2.5.2.3 Where it is not possible to achieve restoration of all systems, partial restorations can be considered, planned as they will operate at a lower capacity level, and key milestones in reinstallation and reconfiguration of systems are defined to ensure effective recovery.	
2.5.3	Monitoring	Monitoring network, systems and service providers during the process of restoring technology infrastructure assets is critical to detect abnormal activities. When appropriate and according to its size, complexity and risks, it is desirable to include in service agreements with the vendor monitoring capabilities during data restoration.	
2.5.4	Validation	Before systems and services return to normal operation, you must validate the integrity of restored IT assets and ensure that they are not compromised, functional and meet security requirements.	
2.5.5	Registration of activities	All actions undertaken from the moment the incident was detected until its final resolution should be documented and recorded, as far as possible, in order to enable its follow-up. Once operations have been recovered, the logs will make it easier to reverse actions taken until pre-incident conditions are restored or troubleshoot if recovery actions are unsuccessful. It will be necessary to register the tools and artifacts, such as scripts,	

		configuration changes among others, used in restoration and recovery for future use or for the improvement of current processes and/or systems.	

6.6 Coordination and Communication

Section 2.6 of "A" 7266 specifies that financial institutions should communicate and coordinate with internal and external stakeholders during the lifecycle of cyber incidents to help them understand and pay attention to cyber incidents. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.6.1	Timely scaling	For timely treatment, the incident must be reported to each stakeholder group without delay, in accordance with the criticality assessment framework and expected escalation levels. It is also important that communication to service providers is defined in service agreements. It is important to provide reasonable assurances to ensure that complete and accurate information is provided in communications for both internal areas and external organizations.	Customers should sign a legally binding service agreement with the service provider and ensure the legality and suitability of the terms of the agreement. In the service agreement, FIs shall agree with the service provider on information security measures to ensure the integrity and accuracy of their information. To cooperate with customers to meet regulatory requirements, HUAWEI CLOUD provides online version of HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed according to the actual situation.
2.6.2	Notification of cyber incidents	2.6.2.1. Relevant information of cyber-incidents should be reported to the authorities as required and in accordance with the deadlines established by the corresponding	FIs should develop a cyber security incident process, which should include requirements and step instructions for notifying and escalation to relevant stakeholders (such as data controllers, data

		regulatory frameworks. To support effective and timely reporting of cyber incidents, they need to develop internal guidelines on when and to whom different types of incidents should be reported. Examples of different types of incidents and reports can be used to improve understanding. 2.6.2.2. Additionally, participants who may be affected by possible disruptions caused by a cyber incident should be informed so that they can activate their own response and recovery plans. Shared information should be accurate, timely, clear and relevant; both internal and external stakeholders should also be kept informed at an appropriate frequency, but without delay should be communicated when urgent. Conditions or restrictions should also be reported at the time of the resumption of critical services. In each message the actions expected from the recipient should be indicated, setting the frequency in advance.	subjects, regulatory agencies, etc.). In order to cooperate with customers to meet the requirements of reporting data loss and breach incidents to relevant stakeholders. HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. According the requirements of laws and regulations, HUAWEI CLOUD timely discloses relevant events, promptly informs customers, and implements emergency plans and recovery procedures to reduce business impact. In addition, HUAWEI CLOUD has established a data breach incident handling mechanism, and the company's legal affairs or local DPO is responsible for identifying data breach-related requirements in applicable laws and regulations. After the incident, the legal affairs or local DPO will approve and report the notification requirements and content.
2.6.3	Communication of the cyber incident to the public	It is necessary that the communication strategy is predefined and a multidisciplinary communication team made up of, among others, representatives of the affected lines of business, human resources, press and communication, legal, technology and cybersecurity, as well as the incident coordinator is recommended. Depending on the type of incident, other specialists may be asked for help. To avoid confusion in communication, the spokesperson will need to consolidate the information and the different relevant aspects of both experts and management, to update the media with	

		consistent information and messages. A strategic use of communication channels such as mainstream media and social media must be promoted.	
2.6.4	Exchange of information	2.6.4.1. It is recommended that organizations share information on cyber threats and cyber incidents, effective cybersecurity strategies and risk management practices, through platforms or by means they deem appropriate to implement. It will be very useful to share technical information, such as indicators of commitment and vulnerabilities that are being exploited, as soon as it is available, ensuring the necessary anonymity to comply with your confidentiality agreements. 2.6.4.2. Communication channels must be formalized and ensure the availability, integrity and confidentiality of the information that is shared. It is also necessary for participants to periodically validate the availability of communication channels and the contact list.	

6.7 Continuous Improvement

Section 2.7 of "A" 7266 specifies the procedures to be considered for improving the capability to respond to cyber incidents based on experience. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.7.1	Initiatives	It is substantial to share knowledge and skills with the other participants, create spaces or forums to discuss incidents and mitigation strategies against cybersecurity	After the incident is handled, FIs should analyze the vulnerabilities and threats caused by cyber security incidents and deploy corresponding control measures according to the results of business Impact analysis

		vulnerabilities and threats. It is important that the authorities work together to promote the exchange of information and good practices. The exchange allows participants to benefit from the information by contributing to mutual understanding and improving response and recovery capabilities.	(BIA). At the same time, FIs shall organize a summary and report on the emergency response process of the incident, analyze the timeliness and effectiveness of the incident handling, and the quality of forensic analysis in the process.
2.7.2	Post-incident analysis	Once the cyber incident is closed, it should be reviewed whether the established procedures were followed and whether the actions taken were effective, as well as: i) the speed of response to security alerts, ii) the opportunity to determine the impact of the incidents and their severity, iii) the quality of the forensic analysis, iv) the effectiveness of the escalation within the entity, and v) the effectiveness of the communication, both internal and external.	
2.7.3	Exercises	The exercises can be both internal and third-party, testing contingency plans and crisis management, the relationship with suppliers or peers, to prepare and improve coordination among the various actors involved. These exercises include different scenarios to validate the effectiveness of coordination of response and recovery activities. In order to improve cyber resilience, the participation of national authorities in these exercises is recommended.	FIs should develop emergency plans and crisis handling procedures, and conduct regular emergency drills according to the plans and procedures to improve the resilience of financial institutions to network security and enhance their emergency response capabilities. If HUAWEI CLOUD is required to participate in an emergency drill, HUAWEI CLOUD will arrange its personnel to meet customers' requirements.

7 Conclusion

This document describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in Argentina and shows that HUAWEI CLOUD complies with key regulatory requirements issued by the BCRA. This aims to help customers learn more about HUAWEI CLOUD's compliance status with Argentina'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 Argentina'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 Argentina's financial industry when using HUAWEI CLOUD.

8 Version History

Date	Version	Description
2024-8	2.1	Routine update
2022-1	2.0	Compliance requirement update
2021-5	1.0	First release