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

Issue 3.0

Date 2024-09-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

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
1.1 Background and Purpose of Publication 1
1.2 Introduction of Applicable Financial Regulatory Requirements in Brazil 1
1.3 Definitions 2
2 HUAWEI CLOUD Security and Privacy Compliance 3
3 HUAWEI CLOUD Security Responsibility Sharing Model 6
4 HUAWEI CLOUD Global Infrastructure 8
5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of CMN Resolution 4.893 and BCB Resolution 85 9
5.1 Cyber Security Policy 9
5.2 On the Contracting of Services of Data processing, Data Storage and Cloud Computing 13
5.3 General Provisions 20
6 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of Brazilian Government Decree 8.771 23
6.1 Network Security 23
6.2 Protection of Records, Personal Data and Private Communications 25
7 Additional Security Measures Available to the Customer 28
8 Conclusion 31
9 Version History 32

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing has become the normal condition of Brazilian financial institutions (FIs). Cloud computing brings great benefits to the development of FIs, but it also creates a complex environment for FIs. To regulate the application of Information Technology (IT) in the financial industry, the National Monetary Council (CMN) and The Central Bank of Brazil (BCB) published a series of regulatory requirements and guidelines, covering cyber security and IT risk management for FIs operating in Brazil. In addition, Decree 8.771 issued by Brazilian government provides guidelines on data security that should be observed by entities who perform data treatment activities, and Brazilian FIs also need to comply with the requirements of the Decree.

HUAWEI CLOUD, as a cloud service provider, is committed not only to helping FIs meet local regulatory requirements, but also to continuously providing them with cloud services and business operating environments meeting FIs' standards. This white paper sets out details regarding how HUAWEI CLOUD assists FIs operating in Brazil to meet regulatory requirements when providing cloud services.

1.2 Introduction of Applicable Financial Regulatory Requirements in Brazil

The National Monetary Council (CMN)

- **Resolution 4.893 of February, 26th 2021**: This Resolution, which came into force on July,01st 2021, sets out the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by FIs licensed by BCB. This Resolution revokes and replaces the Resolution 4.658 of April,26th 2018 and Resolution 4.752 of September, 26th 2019.

The Central Bank of Brazil (BCB)

- **Resolution 85 of April,08th 2021**: This Resolution, which came into force on August,01st 2021, specifies the cybersecurity policies and requirements for data processing and storage and cloud computing services that payment institutions authorized by the BCB shall comply with. This Resolution revokes the Resolution 3.909 of August,16th 2018 and Resolution 3.969 of November,13th 2019.

Brazilian Government

- **Decree 8.771 of May,11th 2016**: This Decree regulates the Law 12.965 of April,23rd 2014 (Internet Civil Framework or "Marco Civil da Internet") and provides the guidelines on data security that should be observed by connection and application provider entities. These guidelines focus on controlling access to personal data and the use of encryption or equivalent protective measures.

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.

- **Service provider**

  An entity, including its affiliate, providing services to a FI under an outsourcing arrangement.

- **Cloud computing**

  Means a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources (for example servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning, and administration on-demand.

- **Content data**

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

2 HUAWEI CLOUD Security and Privacy Compliance

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

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

Example of Huawei Cloud Partial Standard Certification：

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

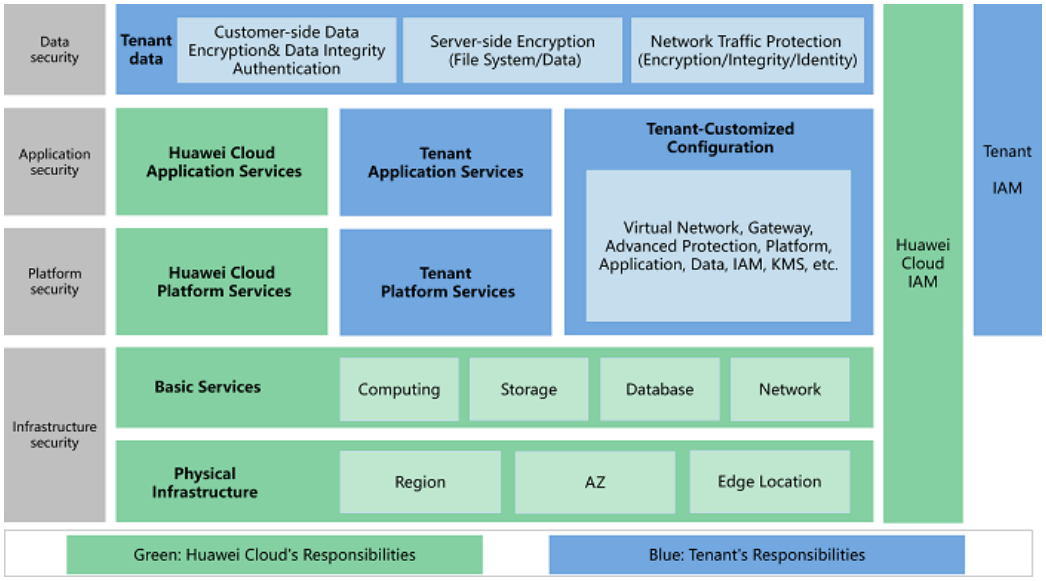
Certification	Description
	TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000. Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.
ISO 20000-1	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO22301	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
ISO27701	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
ISO29151	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD’s implementation of internationally recognized management measures for the entire lifecycle of personal data processing.

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

3 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model



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

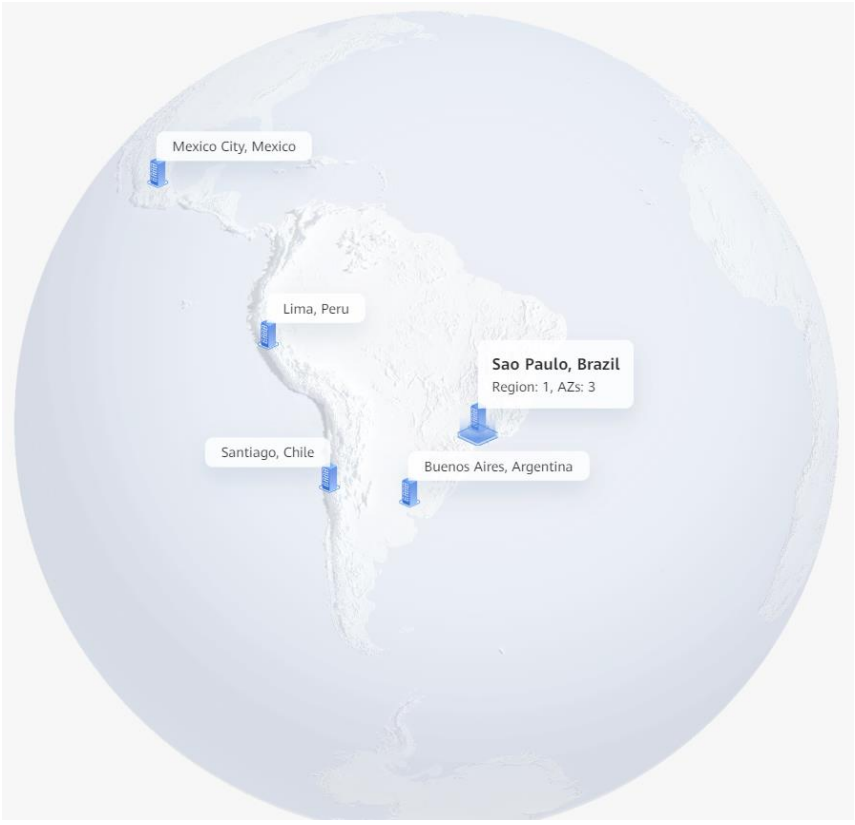
HUAWEI CLOUD: The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also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

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

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

4 HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain. In Brazil, HUAWEI CLOUD has deployed the LA-Sao Paulo1 region, which has three AZs. Customers can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD "**Worldwide Infrastructure**".



5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of CMN Resolution 4.893 and BCB Resolution 85

CMN issued *Resolution 4.893* on February 26th, 2021. The Resolution sets cyber security management requirements for FIs licensed by BCB from the fields of cyber security policy, the contracting services of data processing and data storage and cloud computing, and general provisions.

BCB issued *Resolution No. 85* on April 8th, 2021. The Resolution sets out the cybersecurity policy and requirements for data processing and storage and cloud computing services to be followed by payment institutions authorized by the Central Bank of Brazil.

When FIs are seeking to comply with the requirements stipulated in *Resolution 4.893* and *Resolution No. 85*, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following contents summarize the requirements related to cloud service providers in *Resolution 4.893* and *Resolution No. 85* and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

**Remarks: Except for the different application targets of resolution 4.893 and Resolution No. 85, the article numbers and contents of control requirements related to cloud service providers are almost the same. Therefore, how HUAWEI CLOUD, as a cloud service provider meets and assists FIs to meet these requirements is described together in this chapter.*

5.1 Cyber Security Policy

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2 and 3	Cyber Security Policy Implementation	2. FIs must implement and maintain a cybersecurity policy formulated according to principles and guidelines that seek to ensure the confidentiality,	Customers should develop and implement a cybersecurity policy clarifying the cybersecurity objectives, information security measures, incident management process, business continuity management process, data classification standard, etc. As a cloud service provider, according to ISO 27001, HUAWEI CLOUD has built

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		integrity and availability of data and information systems used. 3. The cyber security policy must comprise, at a minimum: I - the institution's cyber security objectives; II - the procedures and controls adopted to reduce the institution's vulnerability to incidents and to address other cyber security objectives; III - the specific controls, including those directed at information traceability, aiming to ensure the security of sensitive information; IV - recording, analyzing causes and effects, and controlling the impact of events related to the activities of the institution; V - the guidelines to: a) the development of scenarios that reflect incidents considered in business continuity tests; b) the definition of procedures and controls directed at the prevention and treatment of incidents to be adopted by third party providers that handle sensitive data or information, or that are relevant for the institution's operational activities; c) the classification of	a comprehensive 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 focus areas and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the inviolability, integrity, and availability of customer systems and data in one comprehensive effort.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		data and information according to their relevance; d) Define the parameters used to assess the relevance of incidents. VI - Mechanisms to spread a culture of cybersecurity within the institution; VII - Proactively share information about relevant incidents, mentioned in Section IV, with other institutions referred to in Art.01 of the Resolution.	
6, 9 and 10	Plan of Action and Response to Incidents	6. The FIs must establish a plan of action and response to incidents, aiming at the implementation of the cyber security policy. 9. The cyber security policy mentioned in art. 2 and the action plan and response to incidents mentioned on art. 6 must be approved by the board or, in case a board is nonexistent, by the senior management. 10. The cyber security policy and the action plan and response to incidents must be documented and revised at least annually.	Customers should develop a plan of action and response to incidents, and obtain approval from the board of directors, or, in case a board is nonexistent, by the senior management. In addition, customers should regularly update the cybersecurity policy and the action plan. As a cloud service provider: **(1)** HUAWEI CLOUD has developed an internal security incident management mechanism 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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 incidents 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)** HUAWEI CLOUD has formulated various specific contingency plans to deal with complex security risks in the cloud environment. Each year, HUAWEI CLOUD conducts contingency plan drills for major security risk scenarios to quickly reduce potential security risks and ensure cyber resilience when such security incidents occur. 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.

5.2 On the Contracting of Services of Data processing, Data Storage and Cloud Computing

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
12 and 14	Service Provider Evaluation	12. The FIs, prior to contracting relevant data processing, data storage and cloud computing services, must verify the capabilities of service providers to ensure: a) compliance with the laws and regulations in force; b) the institution's access to data and information to be processed or stored by the service provider; c) confidentiality, integrity, availability and recovery of data and information processed or stored by the service provider; d) its adherence to certifications required by the institution in order to perform the services to be contracted; e) the institution's access to reports provided by the specialized independent auditor hired by the service provider, related to the procedures and the controls used in the services to be contracted; f) provision of adequate information and management resources to monitor the services to be contracted;	Customers, prior to contracting relevant data processing, data storage and cloud computing services, must verify the capabilities of service providers, including data security, certifications, auditing reports, service monitoring, data isolation, access control, etc. As a cloud service provider, HUAWEI CLOUD's performance in the aforesaid aspects is as follows: **(1) Compliance with applicable laws and regulations:** The development of HUAWEI CLOUD business follows Huawei's strategy of "one policy for one country/region, one policy for one customer", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the customer is located. HUAWEI CLOUD not only leverages and adopts excellent 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 customers. HUAWEI CLOUD will also openly and transparently tackle cloud security challenges standing should-to-shoulder with customers and partners as well as relevant governments in order to support the security requirements of customers. **(2) Customer's Access Rights:** Customers retain ownership and control of their data. The products and services provided by HUAWEI CLOUD allow customers to determine where their

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		g) the identification and segregation of data pertaining to the institution's clients through physical or logical controls; and h) the quality of access controls aimed at protecting the data and information of the institution's clients. 14. The institution contracting the services mentioned in art. 12 is responsible for the reliability, integrity, availability, security and confidentiality of the services contracted, as well as for compliance with the legislation and regulation in force.	content data will be stored and support users' access to their resources and data on HUAWEI CLOUD. **(3) Data Security:** Data security refers to the comprehensive protection of users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry leading standards for data security lifecycle management and adopt excellent security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, data transmission, data storage, data deletion, and physical destruction of storage media. HUAWEI CLOUD provides customers with effective data protection capabilities to protect their data privacy, ownership and control rights from infringement. For more information on how HUAWEI CLOUD complies with LGPD please refer to our **HUAWEI CLOUD Compliance with Brazil LGPD**. **(4) Certification:** HUAWEI CLOUD has obtained ISO 27001, ISO27701, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. For more information, please refer to "2. HUAWEI CLOUD Security and Privacy Compliance" of this document. **(5) Auditing Reports:** Third-party evaluation companies will regularly conduct security, security adequacy and compliance audits, and issue expert reports on HUAWEI CLOUD. The requirements for obtaining third party audit reports will be committed in the agreement signed according to the actual situation. **(6) Service Monitoring: Cloud Eye Service (CES)** provides users with a

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			robust monitoring platform for **Elastic Cloud Server (ECS)**, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service. **(7) Data Isolation:** HUAWEI CLOUD service products and components have planned and implemented appropriate isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature. **(8) Access Control:** HUAWEI CLOUD's unified **Identity and Access Management (IAM)** provides cloud resource access control for customers. With IAM, the customer administrator can manage user accounts and control the access privileges of these user accounts. When multi-user cooperative operation resources exist in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and assist the security of user accounts by setting a login authentication strategy, password strategy and access control list. Through the above measures, we can effectively control privileges and provide emergency accounts. Customers can also use the **Cloud Trace Service (CTS)** as a supplement to provide operational records of cloud service resources for users to query, and for audit.
15	Communication with Regulators	The contracting of relevant data processing, data storage and cloud computing services must be communicated	Customers, previously to the contracting of relevant data processing, data storage and cloud computing services, must be communicated to the Central Bank of Brazil within ten days after contracting the services. The communication should

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		to the Central Bank of Brazil by FIs.	include the service provider's name, contracting services, as well as a description of the countries and the regions where services may be provided and the data may be stored, processed and managed. The notification sent by FI customers to the Central Bank of Brazil is an independent action of FI customers. But FI customers can use the information provided by HUAWEI CLOUD on the official website and ***HUAWEI CLOUD Customer Agreement*** to meet their requirements.
16	Outsourcing outside Brazil	The contracting of data processing, data storage and cloud computing relevant services provided abroad must fulfill the following requisites: I - the existence of an agreement for exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided; II - the contracting institution must ensure that the provision of the services mentioned in this article does not cause damage to its own functioning neither do they deter the action of the Central Bank of Brazil; III - the contracting institution must define, previously to the contracting, the countries and the regions in each country where the services can be provided and the data	For cloud computing services provided outside Brazil, customers should review the BCB's **list of Memorandums of Understanding (MoU)** with different countries published by the Brazilian Central Bank. This list shows the authorities of the countries that have agreements for exchange of information with BCB. In the absence of an agreement, customers must request an authorization from BCB. In addition, customers must ensure that contracting services will not impede its own functioning neither do they deter the action of the Central Bank of Brazil. Customers must determine the services to be provided, the countries and the regions involved in data processing, and the Business Contingency Plan in the case of its termination. To cooperate with customers to meet regulatory requirements, as a cloud service provider: **(1)** HUAWEI CLOUD will not use customer data for commercial monetization 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 applicable laws and regulations or the binding orders of the government institutions. Moreover, HUAWEI CLOUD conforms to the data protection principles described in *General Data Protection Law* (LGPD) of Brazil. For more information on how HUAWEI CLOUD complies with LGPD please refer to our **HUAWEI CLOUD Compliance with Brazil LGPD**.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		can be stored, processed and managed; and IV - the contracting institution must provide alternatives for business continuity either in the case of impossibility of continuation of the contract or in the case of its termination.	**(2)** 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, Customers can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD **Worldwide Infrastructure**.For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD "**Worldwide Infrastructure**". **(3)** When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD, such as migrating to local data center.
17	Service Agreement	The contracts for the provision of relevant data processing, data storage and cloud computing services must comprise: I - an indication of the countries and the regions where services may be provided and data may be stored, processed and managed;	Customers should sign a legally binding service agreement with the service provider and ensure the legality and suitability of the terms of the agreement. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		II - the adoption of security measures for transmission and storage of the data mentioned in item I; III – the maintenance, while the contract is in force, of data segregation and the access controls to protect customer; IV - the obligation of, in the case of contract termination: a) transfer of the data cited in item I to the new service provider or the contracting institution; b) elimination of the data mentioned in item I by the substituted service provider, after the completion of data transfer mentioned in item ‘a' and the confirmation of the integrity and availability of the received data. V - the access by the contracting institution's to: a) information provided by the service provider, in order to verify the compliance with items I and III; b) information related to certifications and reports provided by the specialized independent audit mentioned in art 12, item II, sub-items “d” and “e”; c) proper information and management resources to monitor the services to 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		provided, mentioned in art. 12, item II, sub-item "f". VI - the obligation of the service provider to notify the contracting institution in case of subcontracting services deemed relevant to the contracting institution; VII - the permission of access by BCB to the contracts and agreements signed for the provision of services, the documentation and information related to the services provided, data stored and information about its processing, backup of data and information, as well as access codes to the data and information; VIII - the adoption of measures by the contracting institution as a result of determinations from BCB; and IX - the obligation of the service provider to keep the contracting institution permanently informed about possible limitations that may affect the services provided or compliance with laws and regulations in force.	

5.3 General Provisions

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
19	Business Continuity Management Policy	FIs must ensure that their risk management policies implemented in conformity with the regulation in force comprise, relating to business continuity: I - the handling of relevant cyber security incidents mentioned in art. 3, item IV; II - the procedures to be followed in case of an interruption of relevant contracted data processing, data storage and cloud computing services, covering scenarios that consider a substitution of the contracted service provider and the re-establishment of the normal operation of the institution; and III - the incidents scenarios considered in the business continuity tests referred to on art 3. Item V, letter “a”.	Customers should establish a business continuity management policy. As a cloud service provider: (1) HUAWEI CLOUD has developed a security event management mechanism and continuously optimizes the mechanism. The security incident response process clearly defines the roles and responsibilities for each activity in the incident response process. The log big data analysis system of HUAWEI CLOUD can quickly collect, process, and analyze massive logs in real time. It can interconnect with third-party security information and event management systems such as ArcSight and Splunk. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems, and threat detection alarm logs of security products and components. It continuously monitors and analyzes security events in real time to ensure timely detection of security events. In addition, Huawei Cloud has a 24/7 professional security incident response team and a security expert resource pool to handle security incidents. HUAWEI CLOUD defines the principles for grading and escalating security incidents, grades the incidents based on the impact of the incidents on customers' services, and starts the customer notification process based on the security incident notification mechanism to notify customers of the incidents. When a serious security incident occurs and has or may have a serious impact on a large number of customers, HUAWEI CLOUD can notify customers of the incident information as soon as possible through bulletins. The notification information includes at least the event description, cause, impact, measures taken by HUAWEI CLOUD, and recommended measures for the customer. After the incident is resolved, HUAWEI CLOUD will provide an incident report to the customer based on

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			the actual situation. (2) To cope with complex security risks in the cloud environment, HUAWEI CLOUD formulates various special emergency plans and performs emergency drills for major security risk scenarios every year to quickly reduce possible security risks and ensure cyber resilience. In addition, according to the requirements of the internal information security management system and business continuity management system, all system documents shall be reviewed and updated as necessary on a regular basis every year. HUAWEI CLOUD maintains a list of contacts who should be contacted in case of emergencies. After receiving a personnel change notification, HUAWEI CLOUD will update the list in a timely manner.
20	Business Continuity Management Procedures	The procedures adopted by FIs for risk management in conformity with the regulation in force must comprise, relating to business continuity: I - the treatment adopted to mitigate the effect of relevant incidents mentioned in item IV, art. 3 and the interruption of relevant data processing, data storage and cloud computing services contracted; II - the deadline stipulated for resumption or normalization of activities or relevant services interrupted, mentioned in item I; III - the timely communication to BCB on the occurrence of relevant incidents and the	Customers must develop a business continuity management mechanism to clarify the recovery target and the minimum recovery strategy and formulate crisis management procedures, including crisis response, handling and notification. As a cloud service provider: **(1)** To provide continuous and stable cloud services to customers, HUAWEI CLOUD has established a set of complete business continuity management systems in accordance with *ISO 22301 - Business Continuity Management International* standards. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. **(2)** HUAWEI CLOUD regularly conducts risk assessment according to the requirements of the internal business continuity management system, identifies and analyses the potential risks faced by key resources supporting the continuous operation of cloud services. HUAWEI

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		interruption of relevant services, mentioned in item I, that configure a crisis situation to the financial institution, as well as procedures for restart of its activities.	CLOUD further considers 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. **(3)** To meet the requirements for notification, HUAWEI CLOUD has developed a complete process for event management and notification. If an event occurs on the HUAWEI CLOUD Base Platform, relevant personnel will analyze the impact of the event according to the process. If the event has or will have an impact on the cloud service customers, HUAWEI CLOUD will start to notify customers of the event. The contents of the notice include but are not limited to description of the event, the cause, impact, measures taken by HUAWEI CLOUD, and measures recommended for customers. The internal customer notification process ensures that HUAWEI CLOUD can promptly notify customers of events with an announcement when serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers.

6 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of Brazilian Government Decree 8.771

Brazilian government issued *Decree 8.771* on May 11, 2016. This Decree sets data protection requirements from the fields of network security, and protection of records, personal data and private communications, etc.

When FIs are seeking to comply with the requirements provided in *Decree 8.771*, 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 *Decree 8.771*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

6.1 Network Security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5	Network Security	The essential technical requirements to the adequate provision of services and applications shall be observed by the responsible for the activities of transmission, switching or routing, in the scope of its respective network, and their purpose is to maintain its stability, security, integrity, and functionality. (1) The essential technical requirements	For the handling of network security issues and extraordinary situations of network jamming, customers should follow the technical requirements that are indispensable to the adequate provision of services and applications to maintain the stability, security, integrity, and functionality. In order to cooperate with customers to meet regulatory requirements, as a cloud service provider: **(1)** HUAWEI CLOUD provides **Advanced Anti-DDoS (AAD)**. To defend against DDoS attacks, HUAWEI CLOUD provides multiple security protection solutions. AAD provides three sub-services: Basic Anti-DDoS, Advanced Anti-DDoS, and Advanced Anti-DDoS. AAD can be used to protect

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		indicated in the lead paragraph are the ones deriving from: I - handling network security issues, such as restriction to the sending of mass messages (spam) and control of denial-of-service attacks; and II - handling exceptional situations of network jamming, such as alternative routes in case of interruptions in the main route and in emergency situations.	HUAWEI CLOUD and non-HUAWEI CLOUD hosts. User can change the DNS server or external service IP address to a high-defense IP address, thereby diverting traffic to the high-defense IP address for scrubbing malicious attack traffic. This mechanism ensures that important services are not interrupted. HUAWEI CLOUD Anti-DDoS attack services provide fine-grained DDoS mitigation capabilities to deal with the likes of Challenge Collapsar attacks and Ping Flood, SYN, UDP, HTTP, and DNS floods. Once a protection threshold is configured (based on the leased bandwidth and the business model), Anti-DDoS will notify the affected user and activate protection in the event of a DDoS attack. **(2)** HUAWEI CLOUD's **Web Application Firewall (WAF)** is an advanced web application firewall service featuring a series of targeted optimization algorithms that give full play to Huawei's extensive experience in network attacks and defense mechanisms. HUAWEI CLOUD's WAF runs on the dual-engine architecture of regular expression rule and semantic analysis to realize high-performance protection against SQL injections, cross-site scripting (XSS) attacks, command and code injections, directory traversals, scanners, malicious bots, web shells, and CC attacks. HUAWEI CLOUD's WAF provides a user-friendly and centralized management interface on which users can configure protection settings based on their service and business requirements, view WAF logs, and resolve false positive events. **(3)** Customers can use **Elastic Load Balance (ELB)** to load balancing between different regions. The ELB automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs. **(4)** Customers can rely on the Region and Availability Zone (AZ) architecture of

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

6.2 Protection of Records, Personal Data and Private Communications

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
13	Access Control	Connection and application providers must observe the following guidelines on security standards when storing, safeguarding and processing personal data and private communications: I - the establishment of strict controls over access to data; by instituting responsibilities for those who have access and exclusive access privileges for certain users; II - the provision of authentication mechanisms for access to records, by using, for example, dual	Customers must develop an access control mechanism to set up the level of access based on the user's responsibilities, adopt secure authentication and data encryption technologies, and record access logs. In order to cooperate with customers to meet regulatory requirements, as a cloud service provider: **(1)** Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Each HUAWEI CLOUD customer has a unique user ID in HUAWEI CLOUD. In addition, HUAWEI CLOUD provides a variety of user authentication mechanisms. • IAM supports the security administrators of customers to set up different password strategies and change cycles according to their needs to prevent users from using simple passwords or using fixed passwords for a long time which will result in account leakage. In addition, IAM

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		authentication systems to ensure the individualization of those responsible for data processing; III - the creation of detailed access logs to connection and applications records. Those records shall contain the time and duration of access, the identity of the official or company appointed administrator involved and the identification of the files accessed. IV - the use of records management solutions through techniques that guarantee the inviolability of the data, such as encryption or equivalent protection measures.	also supports customers' security administrators to set up login strategies to avoid users' passwords being violently cracked or to leak account information by visiting phishing pages. • IAM supports multi-factor authentication mechanism (MFA) at the same time. MFA is an optional security measure that enhances account security. If MFA is enabled, users who have completed password authentication will receive a one-time short message service (SMS) authentication code that they must use for secondary authentication. MFA is used by default for changing important or sensitive account information such as passwords or mobile phone numbers. • If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. **(2)** 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. **(3)** HUAWEI CLOUD has established a sound operation and maintenance account management mechanism. When HUAWEI CLOUD O&M personnel access HUAWEI CLOUD Management Network for centralized management of the system, they need to use the uniquely identifiable employee identity accounts. User accounts are equipped with strong

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			password security policies, and passwords are changed regularly to prevent violent decryption. In addition, HUAWEI CLOUD uses two-factor authentication to authenticate cloud personnel, such as USB key, Smart Card and so on. All operation accounts are centrally managed by LDAP. Centralized monitoring and automatic auditing through a unified operation audit platform to achieve full-process management from user creation, authorization, authentication to authority recovery 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.
16	Disclosure of Security Standards	The information about the security standards adopted by application and connection providers should be disclosed in a clear and accessible way to any interested party, preferably through their web sites, while respecting the right of confidentiality with regard to business secrets.	Customers should disclose the information about the adopted security standards to interested parties. As a cloud service provider: **(1)** HUAWEI CLOUD has published the introduction of the product functions, security features, and used standard technologies on official website. For details, please refer to "**Help Center**" of HUAWEI CLOUD official website. **(2)** HUAWEI CLOUD has obtained ISO 27001, ISO27701, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. 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 Center**".

7 Additional Security Measures Available to the Customer

HUAWEI CLOUD understands customers' cyber security and data protection requirements and provides additional security measures for customers based on its rich cyber security and data security practices and technical capabilities. Additional security measures cover network, database, security, management, and deployment tools. The data protection, data deletion, network isolation, permission management, disaster recovery, and security audit functions of related products help customers enhance content security.

Product Name	Product Introduction	Core Functions
Identity and Access Management (IAM)	IAM provides user account management services suitable for enterprise-level organizational structures and allocates different resources and operation permissions to enterprise users. After being authenticated and authorized by IAM using the access key, users can call APIs to access HUAWEI CLOUD resources. IAM supports hierarchical and fine-grained authorization to ensure that different users of the same enterprise tenant can effectively manage and control cloud resources. This prevents the entire cloud service from being unavailable due to mis operations of a single user and ensures service continuity of tenants.	Outsourcing of data processing, data storage and cloud computing services Protection of records, personal data and private communications
Cloud Trace Service (CTS)	CTS is a multi-dimensional monitoring platform for resources, such as ECSs and bandwidth. CES provides real-time monitoring alarms, notifications, and personalized reports to accurately learn the status of service resources. It should be emphasized that CES monitors infrastructure resource usage data and does not monitor or touch tenant data.	Outsourcing of data processing, data storage and cloud computing services Protection of records, personal data and private communications
Cloud Eye Service (CES)	CES is a multi-dimensional monitoring platform for resources, such as Elastic Cloud Servers (ECS) and bandwidth. CES provides real-time	Outsourcing of data processing, data storage and cloud

Product Name	Product Introduction	Core Functions
	monitoring alarms, notifications, and personalized reports to accurately learn the status of service resources. You can set alarm rules and notification policies to learn the running status and performance of service instances in a timely manner.	computing services
Data Encryption Workshop (DEW)	DEW is a comprehensive cloud data encryption service. It provides services such as Dedicated HSM, key management, credential management, and key pair management, solving problems such as data security, key security, and complex key management. Keys are protected by Hardware Security Modules (HSMs) and integrated with multiple HUAWEI CLOUD services. Users can also use this service to develop their own encrypted applications.	Outsourcing of data processing, data storage and cloud computing services Protection of records, personal data and private communications Cybersecurity
Database Security Service (DBSS)	DBSS is an intelligent database security service. Based on the machine learning mechanism and big data analysis technology, it provides functions such as database audit, SQL injection attack detection, and risky operation identification to ensure the security of databases on the cloud. User behavior discovery and audit, multi-dimensional analysis, real-time alarms, refined reports, sensitive data protection, and audit log backup. The bypass database audit function provided by database audit can audit risky operations in real time and generate alarms. In addition, compliance reports that meet data security standards can be generated to audit internal violations and improper operations of databases and locate and take accountability.	Outsourcing of data processing, data storage and cloud computing services
Host Security Service (HSS)	HSS is a workload-centric security offering designed to address the unique protection requirements of server workloads in modern hybrid cloud, multi-cloud data center infrastructures. It integrates host security, container security, and web page anti-tamper.	Cybersecurity Protection of records, personal data and private communications
Advanced Anti-DDoS (AAD)	The AAD service provides strong assurance for the continuity of important services of enterprises. When your servers are under heavy-traffic DDoS attacks, Advanced Anti-DDoS (AAD) ensures service continuity. Advanced Anti-DDoS uses high-defense IP addresses as proxies to provide services for origin server IP addresses. It diverts malicious attack traffic to high-defense IP addresses for cleaning, ensuring that important	Cybersecurity

Product Name	Product Introduction	Core Functions
	services are not interrupted. Advanced Anti-DDoS serves Internet hosts on HUAWEI CLOUD, non-HUAWEI CLOUD, and IDCs.	
Web Application Firewall（WAF）	WAF detects HTTP/HTTPS requests to identify and block attacks such as SQL injection, cross-site scripting (XSS), web shell upload, command/code injection, file inclusion, sensitive file access, third-party application vulnerability exploits, CC attacks, malicious crawler scanning, and cross-site request forgery. Ensure the security and stability of web services. On the WAF console, add a website and connect it to WAF. Then, WAF can be enabled. After this function is enabled, all public network traffic of your website passes through WAF. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server IP address, ensuring security, stability, and availability of the origin server IP address. WAF can be deployed in cloud mode or exclusive mode.	Cybersecurity
Elastic Load Balance（ELB）	Customers can use the Elastic Load Balance (ELB) service provided by HUAWEI CLOUD to implement load balancing between different regions. A load balancer automatically distributes access traffic to multiple ECSs to balance their service load. It enables you to achieve higher levels of fault tolerance in your applications and expand application service capabilities.	Cybersecurity

8 Conclusion

This white paper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in Brazil and shows that HUAWEI CLOUD complies with key regulatory requirements issued by The National Monetary Council (CMN), The Central Bank of Brazil (BCB) and Brazilian government. This white paper aims to help customers learn more about HUAWEI CLOUD's compliance status with Brazil'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 white paper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of CMN, BCB and Brazilian government on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This white paper is for reference only and does not have any legal effect or constitute any legal advice. Customers should assess their own situation when using cloud services and be responsible for ensuring compliance with relevant regulatory requirements from CMN, BCB and Brazilian government when using HUAWEI CLOUD.

9 Version History

Date	Version	Description
September 2024	3.0	Regulatory update and overall review
April 2022	2.0	Compliance requirement update
December 2020	1.0	First release

