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

Issue 1.0

Date 2020-12-16

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

1.1 Background and Purpose of Publication

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 4,658**: This policy document 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.

The Central Bank of Brazil (BCB)

- **Circular 3,909**: This policy document sets out the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by payment institutions authorized by BCB.
- **Circular 3,681:** This policy document sets out procedures to be adopted by payment institutions authorized by BCB for risk management, governance, the

safeguarding of funds held in payment accounts, as well as for the fulfillment of norms applicable to the institutions that are part of the National Financial System (SFN).

Brazilian Government

- **Decree 8,771**: This policy document provides the guidelines on data security that should be observed by entities who perform data treatment activities. 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**

  Cloud computing refers to 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).

- **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.

HUAWEI CLOUD has obtained 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.

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

Certification	Description
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
ISO 27799:2016	ISO 27799 standard provides guidance for the healthcare industry and its associated agencies on how to better protect the confidentiality, integrity, auditability and availability of personal health information.
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.
M&O certification	Uptime Institute is a globally recognized data center standardization organization and an authoritative professional certification organization. Huawei cloud data centers have obtained the M&O certification issued by Uptime Institute. The M&O certification symbolizes that HUAWEI CLOUD data center O&M management has been leading in the world.
NIST CSF (Cybersecurity Framework)	NIST CSF consists of three parts: standards, guidelines, and best practices for managing cyber security risks. The core content of the framework can be summarized as the classic IPDRR capability model, five capabilities: Identify, Protect, Detect, Response, and Recovery.
PCI 3DS	The PCI 3DS standard is designed to protect the 3DS environment that performs specific 3DS functions or stores 3DS data, and supports 3DS implementation. PCI 3DS evaluates the 3D protocol execution environment, including the access control server, directory server, or 3DS server function. and system components, such as firewalls, virtual servers, network devices, and applications, that are required in and connected to the 3D execution environment; In addition, the process, workflow, and personnel management of the 3D protocol execution environment are evaluated.

Regional standard certification

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

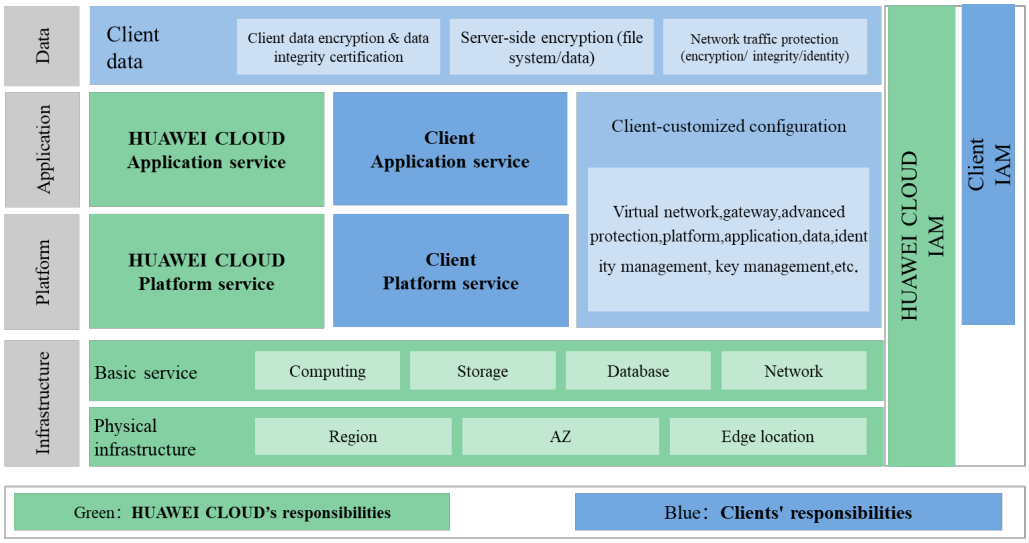
Certification	Description
Cloud Service Security Certification - Cyberspace Administration of China (CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD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

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

3 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model



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

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

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

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

For details on the security responsibilities of both customers 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, 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 4,658 and BCB Circular 3,909

CMN issued *Resolution 4,658* on April 26, 2018, and updated it on September 26, 2019. This policy 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 *Circular 3,909* on August 16, 2018, and updated it on November 13, 2019. This policy sets cyber security management requirements for payment institutions authorized by BCB from the perspectives of cyber security policy, the contracting services of data processing and data storage and cloud computing, and general provisions.

When FIs are seeking to comply with the requirements stipulated in *Resolution 4,658* and *Circular 3,909*, 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 4,658* and *Circular 3,909*, 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 4,658 and circular 3,909, 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, 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 - the record of incidents relevant to the institution's activities, as well as the analysis of their cause and impact	Customers should develop and implement a cybersecurity policy clarifying the cybersecurity objectives, information security measures, event management process, business continuity management process, data classification standard, etc. As a cloud service provider, according to ISO 27001, HUAWEI CLOUD has built 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
		and the control of their effects; 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 data and information according to their relevance;	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 plan of action 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 plan of action 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. In addition, customers should regularly update the cybersecurity policy and the plan of action. 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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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, previously to the contracting relevant services of data processing, data storage and cloud computing, must verify the capabilities of third party 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 third party provider; c) confidentiality, integrity, availability and recovery of data and information processed or stored by the third party 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 third party provider, related to the	Customers, previously to the contracting relevant services of data processing, data storage and cloud computing, must verify the capabilities of third party providers, including data security, certification, obtaining the report, 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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; 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.	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 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. **(4)Certification:** HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications. For more information, please refer to "2.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI CLOUD Security and Privacy Compliance" of this document. **(5)Obtaining the Report:** HUAWEI CLOUD has obtained many authoritative security and privacy protection certificates in the world. 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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			control for customers. With IAM, the customer administrator can manage user accounts and control the access privileges of these user accounts. When multi-user cooperative operation resources exists in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and assist the security of user accounts by setting a login authentication strategy, password strategy and access control list. Through the above measures, we can effectively control privileges and provide emergency accounts. Customers can also use the **Cloud Trace Service (CTS)** as a supplement to provide operational records of cloud service resources for users to query, and for audit.
15	Communication with Regulators	The contracting of relevant services of data processing, data storage and cloud computing must be communicated to the Central Bank of Brazil by FIs.	Customers, previously to the contracting of relevant services of data processing, data storage and cloud computing, should communicate with the Central Bank of Brazil. The communication should include the third party 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 do 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 can be stored, processed and managed; and IV - the contracting institution must anticipate alternatives for business continuity	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 should ensure that contracting services will not impede its own functioning neither do they deter the action of the Central Bank of Brazil. Customers should 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. **(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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		either in the case of impossibility of continuation of the contract or in the case of its termination.	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**". **(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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
17	Service Agreement	The contract of relevant services of data processing, data storage and cloud computing must comprise: I - an indication of the countries and the regions where services may be provided and data may be stored, processed and managed; II - the adoption of security measures for transmission and storage of the data mentioned in item I; III - the segregation of data and the access controls to protect the clients' information while the contract is in force; IV - the obligation of, in the case of contract termination: a) transfer of the data cited in item I to the new third-party provider or the contracting institution; b) elimination of the data mentioned in item I by the substituted third-party provider, after the completion of data transfer mentioned in item 'a' and the confirmation of the integrity and	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 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
		availability of the received data. V - the access by the contracting institution's to: a) information provided by the third-party 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 provided, mentioned in art. 12, item II, sub-item “f”. VI - the obligation of the third-party 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 terms related to the rendering of services, the documentation and information related to the services	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		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 third party 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 treatment of relevant cyber security incidents mentioned in art. 3, item IV; II - the procedures to be followed in case of an interruption of relevant data processing, data storage and outsource of cloud computing services, containing scenarios that consider a substitution of the third party provider and the resumption of the normal operation of the institution; and III - the scenarios of incidents considered in the business continuity tests referred to on art 3. Item V, sub-item “a”.	Please refer to the control domain of **"Plan of Action and Response to Incidents"** under **5.1 Cyber Security Policy** of this document.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
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 interruption of relevant services, mentioned in item I, that configure a crisis situation to the financial institution, as well as procedures for restart of activities.	Customers should 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 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(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 BCB Circular 3,681

BCB issued *Circular 3,681* onNovember 4, 2013. This policy sets FIs' operational risk management requirements from the perspectives of business continuity plan, data security, vulnerability management, change management, problem management, test management, etc.

When FIs are seeking to comply with the requirements provided in *Circular 3,681*, 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 *Circular 3,681*, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(I)	Business Continuity Plan	The risk management structure must provide, with regard to operational risk, at least: I - contingency plan and other mechanisms that guarantee the continuity of the provided payment services.	Customers should develop a business continuity plan to guarantee the continuity of the provided payment services. 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. 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, 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(I)(II)	Data Security	II - protection and security mechanisms for data stored, processed or transmitted; III - protection and security mechanisms for networks, electronic sites, servers and communication channels in order to reduce vulnerability to attacks.	Customers should develop a data security management mechanism to ensure data security during the storage, processing and transmission process. In order to ensure the safe processing of data on the cloud by customers, HUAWEI CLOUD provides layer-by-layer protection for all stages of the data life cycle: **(1) Data creation**: HUAWEI CLOUD provides services on a regional basis, which is the storage location of customer content data. HUAWEI CLOUD will never transfer customer content data across regions without authorization. Customers choose areas based on the principle of nearby access and applicable laws and regulations in different regions when customers use cloud services, so that customer content data is stored in the target location. When customers use cloud hard drives, object storage, cloud databases, container engines and other services, HUAWEI CLOUD uses different granular access control mechanisms such as volumes, buckets, database instances, and containers to enable customers to only access their own data. **(2) Data storage**: Currently, **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, no one except the customer can obtain keys to decrypt data, which supports data security on the cloud.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			(3) Data usage: HUAWEI CLOUD provides customers with services in data access control, security protection, and auditing to help them control data usage and transfer in a fine-grained manner. For more information, please refer to Section 4.5 of "Whitepaper for HUAWEI CLOUD Data Security". **(4) Data transmission**: When customers provide Web site services through the Internet, they can use the certificate management service provided by HUAWEI CLOUD in conjunction with world-renowned certificate service providers. By applying and configuring a certificate for the Web site, the trusted identity authentication of the website and the secure transmission based on the encryption protocol are realized. For customer business hybrid cloud deployment and global layout scenarios, the virtual private network (VPN), cloud dedicated line service, cloud connection and other services provided by HUAWEI CLOUD can be used to achieve business interconnection and data transmission security between different regions. **(5) Data archiving**: HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS**,** **Volume Backup Service (VBS),** and **Cloud Server Backup Service (CSBS)** to back up in-cloud documents, disks, and servers. By integrating the above services with data encryption services, backup data can also be encrypted and stored conveniently and quickly, effectively ensuring the security of backup data. **(6) Data destroying**: If customers want to delete data or data needs to

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			be deleted due to the expiration of a service, HUAWEI CLOUD strictly follows the data destruction standard and agreement with customers to clear the stored data.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(IV)	Logging and Monitoring	IV - procedures to monitor, track and restrict access to sensitive data, networks, systems, databases and security modules.	Customers should develop a monitoring mechanism regarding sensitive data, networks, systems, databases and security modules. In order to cooperate with customers to meet 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 specifications and makes sure that the data is transmitted and preserved accurately and comprehensively. The security of the database itself is strengthened to eliminate risks of counterfeiting, denial, tampering and information leakage. Finally, CTS supports encrypted data storage in OBS buckets. HUAWEI CLOUD uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			The logs support for cybersecurity event backtracking and compliance.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(V)	Vulnerability Management	V - monitoring of data security flaws and complaints from end users in this regard.	Customers should develop a vulnerability management mechanism to monitor data security flaws and complaints from end users in this regard. In order to cooperate with customers to meet regulatory requirements, as a cloud service provider: **(1)**HUAWEI CLOUD's **Vulnerability Scan Service (VSS)** integrates five core functions: Web vulnerability scanning, operating system vulnerability scanning, asset content compliance detection, configuration baseline scanning and weak password detection. It can automatically discover the security risks of websites or servers exposed in the network, and provide multi-dimensional security detection services for businesses on the cloud. **(2)**The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service model, the program ensures rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructures, platforms, applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and technical means. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on clients' services.
4(VI)	Change Management	VI - review of security measures and data confidentiality, especially prior to changes in infrastructure or procedures.	Customers should develop a change management mechanism to review security measures and data confidentiality prior to changes in infrastructure or procedures. HUAWEI CLOUD, as a cloud service provider, is responsible for the management of the infrastructure it provides and the various cloud services of IaaS, PaaS, and SaaS. HUAWEI CLOUD has developed a comprehensive change management process and regularly reviews and updates it. Define the change category and change window, as well as the change notice mechanism, depending on the extent to which the change may affect the business. The process requires that all change requests be submitted to the HUAWEI CLOUD change committee after the change manager makes a judgment. After the review, the network can be changed according to the plan. All changes need to be fully validated before application with tests such as production environment tests, gray release tests, and blue-green deployment. This make that the change committee has a clear understanding of the change, the timeframe, the possible rollback of the change, and all possible impacts.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(VII)	Problem Management	VII - preparation of reports indicating procedures to correct identified flaws.	Customers should develop a problem management mechanism to timely handle and record the identified issues. As a cloud service provider, HUAWEI CLOUD 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.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4(VIII) (IX)	Test Management	VIII - carrying out tests that ensure the robustness and effectiveness of the data security measures adopted; IX - segregation of functions in the information technology environments for development, testing and production.	Customers should develop a test management mechanism to carry out tests that ensure the robustness and effectiveness of the data security measures adopted. In addition, the information technology environments for development, testing and production should be segregated. As a cloud service provider: **(1)** Huawei's development and testing processes follow unified system (software) security development management specifications, and access to various environments is strictly controlled. To meet customer compliance requirements, HUAWEI CLOUD manages the end-to-end software and hardware life cycle through complete systems and processes, as well as automated platforms and tools. The life cycle includes security requirements analysis, security design, security coding and testing, security acceptance and release, and vulnerability management. **(2)** HUAWEI CLOUD takes security requirements identified in the security design stage, penetration test cases from the attacker's perspective, and industry standards, and develops corresponding security testing tools, and conducts multi-round security testing before the release of cloud services to meet the security requirement of the released cloud services. Testing is conducted in a test environment, isolated from the production environment, to avoid the use of production data for testing. If production data is used for testing, it must be desensitized, and data cleaning is required after testing.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4 Sole paragraph	Service Agreement	If payment institutions outsource functions related to the security of the services offered, the respective service provision contract must stipulate that the contractor must: I - comply with the provisions of this article; and II - allow the payment institution's access to data and information about the services provided.	Please refer to the control domain of **"Service Provider Evaluation"** under **5.2 On the Contracting of Services of Data processing, Data Storage and Cloud Computing** of this document.

7 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 policy 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.

7.1 Network Security

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
5	Network Security	The technical requirements that are indispensable 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 indispensable technical requirements indicated in the lead paragraph are the ones deriving from: I - treatment of issues of network security, such as restriction to the sending of mass messages (spam) and control of denial-of-service attacks; and II - treatment of extraordinary situations of network jamming, such as alternative routes in case of interruptions in the main route and in	For treatment of issues of network security 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 customers with two kinds of Anti-DDoS attack services: **Anti-DDoS** and **Advanced Anti-DDoS (AAD)**. Anti-DDoS is a traffic scrubbing service that protects resources such as Elastic Cloud Server and Elastic Load Balance instances from network and application layer distributed denial-of-service (DDoS) attacks. It notifies users of detected attacks instantly, ensures bandwidth availability as well as the stable and reliable running of services. AAD can be used to protect HUAWEI CLOUD and non-HUAWEI CLOUD hosts. User can change the DNS server or external service IP address to a high-defense IP address, thereby diverting traffic to the high-defense IP address for scrubbing malicious attack traffic. This mechanism 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		emergency situations.	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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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.

7.2 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 in the custody, storage and processing of 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 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	Customers should 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 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)

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		involved and the identification 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.	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 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			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, 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 - Security Compliance**".

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
December 2020	1.0	First release

