User Guide to Security of Government Cloud Computing in Brazil

Issue 1.0

Date 2022-09-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview......1

1.1 Background and Purpose of Publication......1

1.2 Introduction of Normative Instruction NO.5 on the Minimum Information Security Requirements for Cloud Computing in Federal Government......1

1.3 Definition......2

2 HUAWEI CLOUD Security and Privacy Compliance......3

3 HUAWEI CLOUD Security Responsibility Sharing Model......8

4 HUAWEI CLOUD Global Infrastructure......10

5 How HUAWEI CLOUD Meets Brazil Normative Instruction NO.5 Requirements...11

6 Conclusion......52

7 Version History......53

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing has become the norm for Brazilian federal government agencies. Cloud computing brings great benefits to the informatization development of federal government agencies, but it also creates a complex environment for federal government agencies. To standardize the use of cloud computing solutions in the government industry, Presidency of the Republic/Office of Institutional Security issued the NORMATIVE INSTRUCTURE NO. 5, which specifies the minimum information security requirements for the use of cloud computing solutions by federal government agencies and entities.

As a cloud service provider, HUAWEI CLOUD is committed to assisting federal government customers in meeting these regulatory requirements and continuously providing government industry customers with cloud services and business operating environments that comply with government industry standards. This document describes the information security regulatory requirements and guidelines that Brazilian federal government agencies or entities usually follow when using cloud services, and details how HUAWEI CLOUD will assist them in meeting the information security regulatory requirements.

1.2 Introduction of Normative Instruction NO.5 on the Minimum Information Security Requirements for Cloud Computing in Federal Government

- **NORMATIVE INSTRUCTURE NO. 5**

The President of the Republic of Brazil/Office of Institutional Security issued NORMATIVE INSTRUCTION NO. 5 on August 30, 2021 (effective as of the date of issuance), which sets out minimum information security requirements for the use of cloud computing solutions by federal government agencies and entities.

As a guide to the minimum information security requirements that federal government agencies or entities that already use or desire to use cloud computing, the Instruction requires federal government agencies or entities to establish cloud computing security management organizations and regulations, and the Instruction provides minimum information security management or technical requirements that federal government agencies or entities should be met when using services provided by cloud computing service providers.

1.3 Definition

- HUAWEI CLOUD

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

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

  Registered users having a business relationship with HUAWEI CLOUD.
- Ocloud Broker

  Ocloud Broker should act as an integrator of cloud computing services between the federal government agency or entity and two or more cloud service providers.

2 HUAWEI CLOUD Security and Privacy Compliance

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

HUAWEI CLOUD has attained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011: “Service Management System (SMS)” .	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: “information security management systems (ISMS)”	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:” cloud computing information security”	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: “business continuity management system”	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 (SOC 1 Type II, SOC 2 Type II, SOC 3)	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 earned SOC 1 Type II, SOC 2 Type II, and SOC 3 certification. Huawei Cloud is the first cloud service provider in the world to meet the SOC 2 requirements for controls related to security, availability, process integrity, confidentiality, and privacy. This certifies that information security controls adopted by Huawei Cloud meet strictest requirements of the internationally recognized standards and also certifies our abilities to provide you with world-class security and privacy protection.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
CSA STAR (Cloud Security Alliance Security, Trust, Assurance and Risk)	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: “personal data protection in the cloud”	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: “the protection of personal identity information”	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: “Privacy Information System Management System”	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017: “personal information data management system”	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.

Regional standard certification

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

Certification	Description

Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
OSPAR certification (Singapore)	OSPAR is an audit report issued by the Association of Banks in Singapore (ABS) to outsourcing service providers. HUAWEI CLOUD passed the guidelines (ABS Guidelines) of the Association of Banks of Singapore (ABS) on controlling the objectives and processes of outsourcing service providers, proving that HUAWEI CLOUD is an outsourcing service provider that complies with the control measures specified in the ABS Guidelines.

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	Classified Cybersecurity Protection issued by China' s Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.

Certification	Description
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	This evaluation evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.

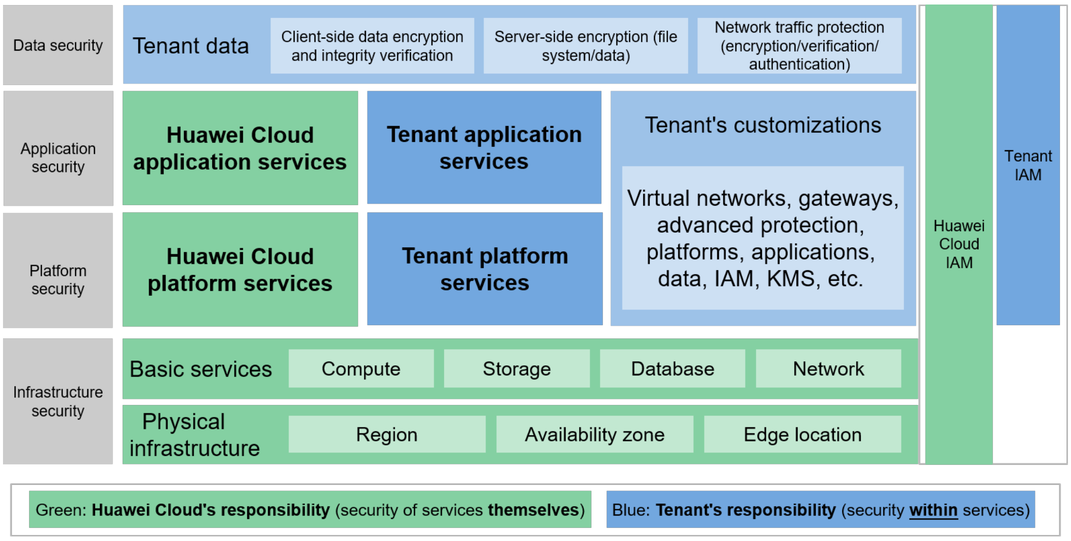
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) (China)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China' s cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS (China)	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification - Cyberspace Administration of China (CAC) (China)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management 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 - Compliance**".

3 HUAWEI CLOUD Security Responsibility Sharing Model

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

Figure 3-1 Responsibility Sharing Model


Data security
Tenant data
Client-side data encryption and integrity verification
Server-side encryption (file system/data)
Network traffic protection (encryption/verification/ authentication)
Application security
Huawei Cloud application services
Tenant application services
Tenant's customizations
Platform security
Huawei Cloud platform services
Tenant platform services
Virtual networks, gateways, advanced protection, platforms, applications, data, IAM, KMS, etc.
Huawei Cloud IAM
Tenant IAM
Infrastructure security
Basic services
Compute
Storage
Database
Network
Physical infrastructure
Region
Availability zone
Edge location
Green: Huawei Cloud's responsibility (security of services themselves)
Blue: Tenant's responsibility (security within services)

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

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

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

For details on the security responsibilities of both agencies and HUAWEI CLOUD, please refer to the **White Paper for HUAWEI CLOUD Data Security** 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). HUAWEI CLOUD customers can flexibly replace computing instances and storage data in multiple geographic regions or between multiple AZs in the same region.. Additionally, Huawei does not touch customer data and strictly follows the local regulations. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD **"Worldwide Infrastructure"**.

5 How HUAWEI CLOUD Meets Brazil Normative Instruction NO.5 Requirements

Normative Instruction NO.5 specifies the minimum information security requirements for the use of cloud computing solutions by federal government agencies or entities. When the federal government agencies comply with the requirements of the Normative Instruction NO.5, HUAWEI CLOUD, as a cloud service provider, may participate in the activities covered by the requirements. The following sections summarize the control requirements related to cloud service providers in the Instruction and describe HUAWEI CLOUD as a cloud service provider, how to assist federal government agencies or entities in meeting these control requirements.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .13	Requirements For Safe Adoption of Cloud Computing: Management of Identities and Registrations (logs).	In relation to the management of identities and records, the organs or entities shall at least: I - adopt a federated identity standard to allow the use of single sign-on technology in the authentication process of its users in the cloud service provider; II - deny the cloud service provider permission to use and direct access to the authentication environment of the agency or entity; III - adopt, according to the level of criticality of the information, the use of single sign-on technology, which must be accompanied: (a) multi-factor authentication; or (b) another alternative that increases the degree of security in the authentication process of its users in the cloud service provider; IV - require the cloud service provider to: (a) record all cyber access, incidents and events, including information about sessions and transactions; and (b) store, for a period of one year, all records referred to in point (a); V - store the records of all cyber accesses, incidents and events, including information about sessions and transactions, for five years in the cloud	Customers should apply Identity Federation Multi-factor authentication, and Single Sign-on technology, and customers are required to store all cyber access and event records in a controlled environment for 5 years. It's up to them to decide whether to store it in the cloud. As a cloud service provider, HUAWEI CLOUD provides the following functions to meet customers' identity management requirements: 1. Provides **Identity and Access Management (IAM)** to manage user accounts that use cloud resources. 1. IAM is a user account management service designed for enterprises that allocates resources and operation permissions to enterprise users in a differentiated manner. Once IAM has authenticated and authorized these users, they can use an access key to access Huawei Cloud resources through APIs. 2. If the customer has a secure and reliable external identity authentication service provider, the customer can map external users authenticated by IAM to temporary users on HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. 3. IAM supports hierarchical fine-grained authorization to ensure that the various users who are part of an

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		service provider's environment or in its own controlled environment, at the discretion of the contracting body or entity; VI - keep in its own environment controlled, for a period of five years, the records of all cyber accesses, incidents and events, including information about sessions and transactions received from the cloud service provider; and VII - empower the security team to access and use the records generated by the cloud service provider.	enterprise tenant use cloud resources as authorized. This authorization scheme prevents users from exceeding the scope of their permissions and ensures the continuity of tenant services. 1. HUAWEI CLOUD supports single sign-on (SSO) for identity authentication. In an environment where multiple systems coexist, a user's login can be trusted by all other systems. 2. Multi-factor authentication (MFA): 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 SMS authentication code that they must use for secondary authentication. IAM is used by default for changing important or sensitive account information such as passwords or mobile phone numbers. 3. As a cloud service provider, HUAWEI CLOUD has developed log management regulations to store all platform-side cyber records for one year. At the same time, the instruction requires agencies to store all network access and event records in a controlled environment for five years, at their discretion, in a cloud environment. To help customers meet log management and

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			supervision requirements, HUAWEI CLOUD provides **Log Tank Service (LTS)** to collect, query, and dump logs in real time. Logs can be stored for a long time. After the log data of hosts and cloud services is reported to the LTS, the storage duration can be set from 1 to 30 days. The log data that exceeds the storage duration will be automatically deleted. For the log data that needs to be stored for a long time (log persistence), the LTS provides the dump function. Logs can be dumped to OBS and DIS for long-term storage.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .14	Requirements For Safe Adoption of Cloud Computing: Cryptographic Resources	In relation to the need for the use of cryptographic resources, organs or entities shall at least: I - verify that the organization's data is being processed and stored in accordance with the legislation; II - analyze the need to encrypt data based on legal requirements, risks, level of criticality, costs and benefits; and III - use, where possible, hardware-based encryption keys.	Customers should evaluate the necessity for data encryption and use secure encryption technologies to encrypt the data. Currently, HUAWEI CLOUD **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 **Data Encryption Workshop (DEW),** which provides full-lifecycle key management. DEW is a comprehensive cloud data encryption service. It provides functions such as dedicated encryption, key management, and key pair management. It uses Hardware Security Module (HSM) to protect the security of keys. DEW can be integrated with other Huawei Cloud services to meet your needs for various encryption scenarios. Users can also use this service to develop their own encryption applications. Without authorization, no one except the customers can obtain keys to decrypt data, which supports data security on the cloud.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .15	Requirements For Safe Adoption of Cloud Computing: Data Segregation and Logic Separation	In relation to data segregation and logical separation in cloud computing environments, agencies or entities, together with the cloud service provider, should establish at least the following actions: I - ensure that the contracted environment is protected from external users of the cloud service and unauthorized persons and implement information security controls in order to provide adequate isolation of resources used by the different organs or entities of the federal public administration and by other users of the cloud service; II - ensure that appropriate logical segregation of virtualized application, operating systems, storage and network data is applied in order to establish the separation of resources used; III - ensure the separation of all resources used by the Cloud Service Provider from those resources used by the internal administration of the agency or entity; and IV - assess the risks associated with running proprietary software to be installed in the cloud service.	Customers should ensure that the cloud service provides effective data isolation and logical isolation before using a cloud service. As a cloud service provider, HUAWEI CLOUD provides logical isolation, data isolation, and separation of services from management and O&M to help customers meet the following requirements: **Logical Isolation:** HUAWEI CLOUD' s Unified Virtualization Platform (UVP) abstracts physical server resources such as CPU, memory, and input/output (I/O) resources, and converts them into a pool of logical resources that can be centrally managed, flexibly scheduled, and dynamically assigned. Based on the logical resources, the UVP provisions on a single physical server a number of VM execution environments, which run concurrently but are isolated from each other. The UVP, which directly runs on physical servers, supports virtualization capabilities and provides execution environments for VMs. The UVP uses technologies such as CPU isolation, memory isolation, and I/O isolation to isolate the virtual host OS from the guest VM OS. In addition, the UVP uses the Hypervisor to make the virtual host OS and the guest VM OS run with different sets of permissions, ensuring platform resource security. **Data Isolation:** HUAWEI CLOUD facilitates data

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer-3 network. Tenants can control their own virtual network construction and configuration. a tenant's VPC can be connected to the tenant' s enterprise network traditional data center using VPN or Direct Connect service such that tenant 's applications and data residing in its internal network can be seamlessly migrated to the tenant' s VPC. On the other hand, the Access Control List (ACL) and security group function of the VPC can be used to configure network security and access rules as per the tenant' s specific requirements for finer-grained network segregation. **Separation of management, Service and O&M:** To ensure that services run by tenants do not affect HUAWEI CLOUD administrative operations and that devices, resources, and traffic are properly monitored and managed, different communication planes have been designed and built into Huawei Cloud' s network based on their different business functions, security risk levels, and access privileges. They include the tenant data plane, service control plane, platform OM plane, Baseboard Management Controller (BMC) management plane, and data storage plane. This ensures that network traffic for different business purposes

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			is reasonably and securely kept in separate lanes, which helps achieve separation of duties, roles, and responsibilities.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .16	Requirements For Safe Adoption of Cloud Computing: Cloud Management	In relation to cloud management, agencies or entities shall at least: I - empower the team responsible for this management in the technologies used by the cloud service provider; II - require the cloud service provider to document and communicate its information security resources, roles, and responsibilities for the use of its cloud services; III-develop an array of responsibilities that includes own obligations and responsibilities; and IV - develop an incident handling process with the cloud service provider and communicate it to the team responsible for cloud management.	The customer should develop an incident handling process. The responsibility sharing model specifies the responsibilities of HUAWEI CLOUD and HUAWEI CLOUD tenants. The security responsibility of HUAWEI CLOUD is to ensure the security of the IaaS, PaaS, and SaaS cloud services provided by HUAWEI CLOUD. HUAWEI CLOUD tenants are responsible for the security and configuration of the cloud. As a cloud service provider, HUAWEI CLOUD manages vulnerabilities based on its vulnerability management system to ensure that vulnerabilities on self-developed and third-party infrastructure, platforms, application layers, cloud services, and O&M tools are detected and fixed within the time specified in SLA. This reduces risks caused by malicious exploitation of vulnerabilities and adverse impacts on customers' businesses. For vulnerabilities that involve the cloud platform and customers' businesses, HUAWEI CLOUD will push the vulnerability mitigation and recovery suggestions and solutions to end users and customers in a timely manner after making sure that no high attack risks will be caused by proactive disclosure. HUAWEI CLOUD will face the challenges brought by the security vulnerabilities together with customers.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			HUAWEI CLOUD also defines service levels for different products to provide users with high availability service commitments. For details, see **HUAWEI CLOUD Service Level Agreement.** 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.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .18	Requirements For Safe Adoption of Cloud Computing: Data in Brazil	The data, metadata, information and knowledge produced or maintained by the agency or entity, transferred to the cloud service provider, must be hosted in Brazilian territory, observing the following provisions: I - at least one updated backup copy must be kept in Brazilian territory; II - the information without access restriction may have updated backup copies outside the Brazilian territory, according to applicable legislation; III - the information with restricted access provided for in the legislation and the preparatory document not provided for in item II of caput art. 17, as well as its updated backup copies, may not be processed outside the Brazilian territory, according to applicable legislation; and	Customers should ensure that restricted data can only be processed within Brazilian territory and data transferred to the cloud service provider must have at least one up-to-date backup of the data on Brazilian territory. HUAWEI CLOUD has established a data center in S ã o Paulo. Customers can migrate data to the cloud in Brazil. For details, see **"Worldwide Infrastructure"**. In addition, HUAWEI CLOUD provides **Cloud Backup and Recovery (CBR),** CBR lets you back up cloud servers, disks, and on-premises VMware virtual environments with ease. CBR protects your services by ensuring the security and consistency of your data. HUAWEI CLOUD complies with the Brazil LGPD. For details, see **HUAWEI CLOUD Compliance with Brazil LGPD**

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .19	Requirements For Safe Adoption of Cloud Computing: Specific Contract Clauses	Art. 19. The contractual instrument to be signed with a cloud service provider for the provision of the cloud computing service shall contain devices dealing with the requirements set out in Art. 10 to Art. 18 and at least the following security procedures: I - confidentiality term that prevents the cloud service provider from using, transferring and releasing data, systems, processes and information from the body or entity to national, transnational, foreign, countries and foreign governments; II - guarantee of the exclusive rights, by the body or entity, over all information processed during the contracted period, including any available copies, such as backups of security; III - prohibition of the use of information from the agency or entity by the cloud service provider for advertising, optimization of artificial intelligence mechanisms or any unauthorized secondary use; IV - compliance of the cloud service provider's information security policy with Brazilian legislation; V - full return of data, information and systems in the custody of the cloud service provider to the contracting bodies or	The customer should sign a legally binding contract with the cloud service provider when using cloud services. The contract should contain confidentiality clauses and prohibit the cloud service provider from using customer data. 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. HUAWEI CLOUD Customer Agreement contains confidentiality clauses that specify confidentiality obligations of all parties. HUAWEI CLOUD will not access or use the customer's content and will not use the customer's data again without authorization. HUAWEI CLOUD Information Security Policy: 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

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		entities at the end of the contract; VI - elimination, by the cloud service provider, at the end of the contract, of any data, information or system of the body or entity in its custody, in the condition of legislation that deals with the mandatory retention of data; and VII - guarantee of the right to forget for personal data, pursuant to Art. 16 of Law No. 13,709 of August 14, 2018 - LGPD.	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. 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. When a customer initiates a data deletion operation or if the data needs to be deleted due to the expiration of the service, HUAWEI CLOUD will strictly follow data destruction standards, as well as agreements with customers, delete the stored customer data. HUAWEI CLOUD complies with the LGPD to ensure the right to forget for personal data. For details, see **White Paper for HUAWEI CLOUD Privacy Protectionr**.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .20	Requirements For Safe Adoption of Cloud Computing: Requirements to Cloud Service Providers	In order to be enabled to provide cloud computing services to federal government agencies or entities, the cloud service provider must meet at least the following requirements: I - to have a risk management methodology, developed in accordance with best practices and legislation, as well as to carry out the risk management described in item II of Art. 11;	The customer should determine whether the cloud service provider has developed a cyber risk management mechanism and has risk management capabilities when using cloud services. HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		II - implement practices for strengthening virtualization mechanisms, which should include at least the following procedures: (a) disable or remove all unnecessary interfaces, ports, devices, or services performed by the operating system; (b) securely configure all network interfaces and virtual storage areas; (c) establish limits for the use of virtual machine resources (Virtual Machine - VM); (d) keep all operating systems and applications running on the virtual machine in their most current versions; (e) validate the integrity of cryptographic key management operations; f) have controls that allow authorized users of the agency or entity to access the administrative access records of the virtual machine monitor - Hypervisor ; g) enable the full registration of hypervisor ; and h) support the use of trusted VM machines provided by the agency or entity that comply with the network strengthening policies and practices required of the cloud service provider;	The customer should confirm that the cloud service provider implements enhanced virtualization mechanisms when using cloud services. As a cloud service provider, HUAWEI CLOUD provides the **Host Security Service (HSS)** to help customers perform automatic baseline check. HUAWEI CLOUD provides the following methods to enhance the virtualization mechanism: **Port management:** HUAWEI CLOUD provides port or interface management capabilities, disables high-risk ports and remote management ports, configures VPCs to isolate networks, configures ACL rules of VPC subnet, and configures security group rules for VPC peering links. VM usage restriction: Resource monitoring can be enabled on VMs to monitor VM resource usage and generate alarms. **Vision update:** HUAWEI CLOUD periodically update and maintain public images, including applying security patches on them as required, and provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. **Encryption key integrity verification:** API requests must be signed with an access key to manage HUAWEI CLOUD resources using O&M tools or API commands by Enterprise administrators. Signature information is verified by the API gateway. Digital signatures and

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			timestamps prevent requests from being tampered with and protect against replay attacks. **Manage Access records:** HUAWEI CLOUD **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. **Hypervisor logging:** Hypervisor is a software layer that runs between the underlying physical server and the operating system. It allows multiple operating systems and applications to share hardware and can also be a virtual machine monitor. When the server starts and runs the Hypervisor, it loads the operating systems of all VM clients and allocates the appropriate amount of memory, CPU, network, and disk to each VM. HUAWEI CLOUD has enabled complete Hypervisor logging to monitor VM usage and provide information support for cloud O&M. **Trusted VMs：** **Image Management Service(IMS)** provides full-lifecycle management of private images, including creating private images, copying, sharing, or exporting private images. Customers can select

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			a proper method based on site requirements and migrate services to the cloud based on peripheral services such as ECSs and object storage.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		III - in relation to identity and record management: (a) to have access control procedures that address the transition between roles, limits and controls of user privileges and controls for the use of user accounts; (b) impose authentication mechanism that requires minimum size, complexity, duration and history of access passwords; (c) support single sign-on technology for authentication; (d) support multi-factor authentication mechanisms or other alternative that increases the degree of security in the authentication process of users of the agency or entity in the cloud service provider, according to the level of criticality of the information; (e) allow the agency or entity to manage its own identities, including creation, update, deletion and suspension in the environment provided by the cloud service provider; and (f) meet the legal requirements, security best practices and other criteria required by the agency or entity in its authentication, access control, accounting and registration processes (format, retention and access);	When using cloud services, the customer should confirm that the cloud service provider establishes an access control management mechanism, sets user rights that match responsibilities, adopts secure identity authentication and data encryption technologies, and records user access in logs. HUAWEI CLOUD provides the following identity and record management capabilities: HUAWEI CLOUD provides IAM to manage user accounts that use cloud resources. In addition to password authentication, IAM supports multi-factor authentication. Customers can choose whether to enable MFA. 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, resulting 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 hierarchical fine-grained authorization to ensure that the various users who are part of an enterprise tenant use cloud resources as authorized. This authorization scheme prevents users from exceeding the scope of their

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			permissions and ensures the continuity of tenant services. HUAWEI CLOUD supports single sign-on (SSO) for identity authentication. In an environment where multiple systems coexist, a user's login can be trusted by all other systems.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		IV - regarding the security of web applications made available in the cloud environment: (a) use firewalls specialized in the protection of systems and applications; (b) develop web codes in compliance with safe development best practices and existing regulations; (c) use best practices for operating system and application security; (d) periodically carry out network and application penetration tests; and (e) have a vulnerability correction program;	When using the cloud service, the customer should confirm that the cloud service provider provides security for web applications in the cloud environment, 1. HUAWEI CLOUD provides **Web Application Firewalls (WAF)** to fend off web attacks such as layer 7 DDoS, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), attacks targeting component-specific vulnerabilities, and identity impersonation. The WAF primarily protects public-facing web-based application services and systems in the DMZ zone. 2.HUAWEI CLOUD strictly complies with the secure coding specifications released by HUAWEI. Before they are onboarded, Huawei Cloud service development and test personnel are all required to learn corresponding specifications and prove they have learned these by passing examinations on them. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding.4.The security

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			baseline is the minimum security guarantee for an information system. The cloud security baseline is the basic security guarantee for the cloud environment and is the basis for security protection. If cloud services do not meet the security baseline requirements, cloud services and assets will face great security risks. 3.HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, check, and resolve security threats to ensure the security of cloud services. According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity, etc. 4.HUAWEI CLOUD security technical team is responsible for implementing security quality assurance and security assessment, conducting

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			internal and third-party penetration tests and security assessment, and monitoring, checking, and resolving security threats. 5.HUAWEI Product Security Incident Response Team(PSIRT) has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD 's self-service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on inhouse-developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		V - have business continuity management and change management processes, in accordance with existing regulations and best practices in these areas; VI - have a disaster recovery plan that establishes procedures for recovering and restoring platform, infrastructure, applications and data after data loss incidents;	When using cloud services, the customer should confirm that the cloud service provider has established a business continuity management mechanism and change management procedure. As a cloud service provider, HUAWEI CLOUD not only provides high availability infrastructure, redundant data backup, and availability zone DR, but also develops business continuity plans and disaster recovery plans and periodically tests them. **Business continuity management :**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. **Change management processes :** HUAWEI CLOUD has developed a comprehensive change management process and regularly reviews and updates

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			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. **Disaster recovery plan**: HUAWEI CLOUD also develops a disaster recovery plan and periodically tests it. For example, if the cloud platform infrastructure and cloud services in a geographical location or region are offline, simulate a disaster, and perform system processing and transfer according to the disaster recovery plan to verify the services and operation functions of the faulty location. The test results will be annotated, recorded, and archived for continuous improvement of the plan.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		VII - establish a secure communication channel using at least Secure Sockets Layer/Transport Layer Security (SSL/TLS) ;	The customer should confirm that the cloud service provider uses Secure Sockets Layer/ Transport Layer (SSL/TLS) to establish secure communication channels when using cloud services. HUAWEI CLOUD provides SSL/TLS encryption capabilities: Both REST and Highway modes support TLS 1.2 for data in transit encryption and X.509 certificate-based identity authentication of destination websites. **TLS capability:** HUAWEI CLOUD supports data transmission in REST and Highway modes. In REST mode, a service is published to the public as a RESTful service and the initiating party directly uses an HTTP client to initiate the RESTful API for data transmission. In Highway mode, a communication channel is established using a high-performing Huawei-proprietary protocol, which is best suited for scenarios requiring especially high performance. **TLS capability:** The SSL Certificate Management service is a one-stop-shop type of X.509 certificate full lifecycle management service provided to our tenants by Huawei Cloud together with world-renowned public certificate authorities (CA). It ensures the identity authentication of destination websites and secure data transmission.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		VIII - use a secure encryption standard, according to international standard recognized accepted, that can be implemented with encryption keys generated and stored by the agency or entity;	The customer should encrypt data using international standard encryption algorithms and key management mechanisms, and keep relevant keys properly when using cloud services. Huawei Cloud provides the Data Encryption Service (DEW) for customers. The DEW key management function enables you to centrally manage keys throughout the lifecycle. Without authorization, no one except the customer cannot obtain a key to decrypt data, ensuring data security on the cloud. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. Huawei Cloud uses the hardware security module (HSM) to create and manage keys for customers. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, helping users meet data compliance requirements and prevent intrusion and tampering. Even HUAWEI O&M personnel cannot have access to customer root keys. DEW allows customers to import their own keys as Customer Master Keys (CMK) for unified management, facilitating seamless integration and interconnection with customers' existing services. In addition, HUAWEI CLOUD uses customer master key online redundancy storage, multiple physical offline

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			backups of root keys, and periodic backups to ensure key persistence.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		X - in relation to data segregation: (a) isolate, using logical separation, all data and services of the body or entity of other cloud service customers; (b) segregate traffic management traffic from the agency or entity; and (c) implement safety devices between zones;	The customer should confirm the data isolation capability of cloud services when using cloud services. HUAWEI CLOUD uses technologies such as VPC to isolate services and data of tenants on the cloud. HUAWEI CLOUD facilitates data isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer-3 network. On the other hand, the ACL and security group function of the VPC can be used to configure network security and access rules as per the tenant' s specific requirements for finer-grained network segregation. To ensure that services run by tenants do not affect HUAWEI CLOUD administrative operations and that devices, resources, and traffic are properly monitored and managed, different communication planes have been designed and built into Huawei Cloud' s network based on their different business functions, security risk levels, and access privileges. They include the tenant data plane, service control plane, platform OM plane, Baseboard Management Controller (BMC) management plane, and data storage plane. This ensures that network traffic for different business purposes is reasonably and securely kept in separate lanes, which helps achieve separation of

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			duties, roles, and responsibilities. A HUAWEI CLOUD data center, unlike a traditional IT data center, requires different mechanisms to achieve security zoning and network segregation. Just firewalls alone are inadequate. The adoption of newer, more innovative technologies such as software-defined perimeter (SDP) is inevitable. Furthermore, trust boundaries and perimeters are everywhere, and are no longer defined at the network layer only. Instead, they have moved up from network layer to the platform layer and application layer, and even all the way up to the user and identity layer, all of which require proper access control.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		XI - have procedures in relation to the disposal of information and data assets, which ensure: (a) safely sanitise or destroy existing data on discarded devices through the use of methods that comply with established standards for conduct and best practices; (b) safely destroy information assets at the end of the life cycle or considered unusable, with the provision of a Certificate of Electronic Equipment Destruction (CEED) and discriminate the assets that have been recycled, as well as the weight and types of materials obtained as a result of the destruction process; and c) store, in a safe way, information assets to be discarded, in an environment with controlled physical access, with record of all movement of input and output of devices;	The customer shall confirm that the Cloud Service shall have procedures in place for the disposal of information and assets when using the cloud service. HUAWEI CLOUD has developed a sound media management process for storage media that stores customer content data to ensure the security of the data stored in the media. When a customer initiates a data deletion operation or if the data needs to be deleted due to the expiration of the service, HUAWEI CLOUD will strictly follow data destruction standards, as well as agreements with customers, delete the stored customer data. Specific practice is: Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored. At the end of the lifecycle, HUAWEI CLOUD will degauss the physical devices and then destroy them. After media destruction, Huawei can provide a destruction certificate (COD) and obtain

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			waste classification and weight information.
		XII - immediately notify organs or entities of cyber incident against the services or data in their custody;	When a cyber incident occurs, the cloud service provider shall immediately notify the institution or entity. 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.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		XIII - have procedures necessary for the preservation of evidence, according to legislation; and	Given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has comprehensive security log management requirements, security event grading and handling processes and a professional security incident response team available 24*7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD has established a forensic investigation management mechanism in accordance with legal requirements and formulated a standardized forensic process to support forensic investigations of security incidents.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		XIV - demonstrate compliance with cloud security standards, through annual Service and Organization Controls 2 (SOC 2) audit , conducted by an independent auditor, with the submission of type I and type II reports.	HUAWEI has set up a dedicated security audit team to periodically review compliance with security laws and regulations worldwide as well as internal security requirements. The team dedicates over ten members to perform a two-month long annual audit on Huawei Cloud operations worldwide, paying close attention to such Huawei Cloud aspects as legal, regulatory, and procedural compliance; business goal and milestone accomplishment; integrity of decision-making information; and security O&M risks. Audit results are reported to HUAWEI' s Board of Directors and executive management, who ensure that any and all identified issues are properly resolved and closed. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications and is audited by third parties every year. HUAWEI CLOUD has completed the SOC audit project and adopted the five control attributes of SOC 2 Type II . (Security, Availability, Process Integrity, Confidentiality, Privacy), which complies with cloud security standards. SOC 2 Type II has the same opinion as SOC 2 Type I reports, and SOC 2 Type II adds more opinions on operational effectiveness than SOC 2 Type I to achieve relevant control objectives.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			If necessary, government agencies can apply to HUAWEI CLOUD for a copy of the SOC2 Type II audit report through official channels.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .22	Using Decloud Brokers	If the agency or entity hires through the cloud broker multi-cloud management platform to perform procedures for provisioning and orchestration of the environment, it is necessary that the tool has at least: I - regarding multi-cloud provisioning and orchestration features: (a) a single integrated provisioning portal for the end user; (b) the use of provisioning models; (c) secure automation of simultaneous provisioning and use, where it is, open source and interoperable tools; (d) event-based orchestration workflows; and (e) integrated secure infrastructure creation solutions by code - IaaC;	HUAWEI CLOUD provides **HUAWEI CLOUD Stack**, it is cloud infrastructure on the premises of government and enterprise customers, offering seamless service experience on cloud and on-premises. ManageOne is a multi-cloud management platform in the HUAWEI CLOUD Stack solution. It provides a unified comprehensive resource allocation portal for end users and provides AutoOps for multi-cloud configuration and orchestration. AutoOps is an O&M automation platform built based on the agile O&M concept. It provides full-stack automatic O&M capabilities from infrastructure to service applications. Builds a rich O&M operation library, flexibly orchestrates O&M processes, standardizes various O&M scenarios, and executes O&M operations or processes in batches on a scheduled or immediate basis. It can be expanded on demand based on enterprises' O&M requirements, minimizing labor costs, reducing management risks, and eliminating boring repetitive work. Improve O&M efficiency and satisfaction. AutoOps supports infrastructure as code IaaC. Minimum unit for automatic execution, which consists of parameters and scripts. The O&M script of a single atom is encapsulated into an O&M operation. Each O&M operation completes a specific O&M action. The system

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			supports a built-in operation library and a customized operation library. The built-in operation library contains various routine O&M operations. The customized operation library helps users expand customized O&M operations based on O&M scenarios.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		II - in relation to multi-cloud monitoring and analysis features: (a) monitoring reports on the performance of resources in the cloud; (b) collection and monitoring of records; and (c) alert monitoring procedures;	The HUAWEI CLOUD ManageOne multi-cloud management platform provides the following monitoring and analysis functions: **Monitoring and analysis:** You can use the monitoring dashboard to collect statistics and health status of alarms, resources, and applications. The monitoring dashboard can centrally monitor capacity, alarms, and resources in real time. It also provides various chart components and comprehensive O&M data, helping O&M personnel build customized monitoring based on customized charts to meet routine O&M requirements. **Alarm monitoring:** When alarms or exceptions occur, risks can be quickly identified to ensure normal system running. **Monitoring and recording:** HUAWEI CLOUD ManageOne provides log management, which consists of unified log management and ManageOne Maintenance Portal log management. It provides efficient and secure log collection, query, storage, download, configuration, and management functions, helping O&M personnel easily cope with O&M scenarios such as log collection and query.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		III - in relation to multi-cloud inventory and classification features: (a) inventory of resources in the cloud; (b) security procedures for configuring resources in the multi-cloud management platform; and (c) detection of unlabeled features; and	HUAWEI CLOUD ManageOne multi-cloud management platform provides a unified resource management center. **Resource management center:** Tenants can use the resource center to quickly manage resources applied for on the cloud platform and view resources in multiple dimensions, improving resource management efficiency. **Classification:** Administrators define different tags and bind tags to resources to classify resources. A tag is a tool used to mark the classification or content of an object, which facilitates locating and locating the object. **Security program:** A comprehensive security control mechanism is provided. Security policies can be defined in advance, security reminders are provided in the event, and audits can be performed after the event, preventing manual operation security risks.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
		IV - regarding security, compliance and identity management functionalities: (a) single sign-one multi-factor authentication mechanisms of cloud platforms; (b) secure management of users and user groups; (c) security management of resources; (d) notifications of multichannel alert events; (e) identity and access management - IAM; and (f) cloud platform activity logs.	The HUAWEI CLOUD ManageOne multi-cloud management platform provides security, compliance, and identity management functions. **Identity management:** Based on the unified architecture and IAM of HUAWEI CLOUD Stack and HUAWEI CLOUD, ManageOne provides a new hybrid cloud implementation, that is, the federated cloud. The federated cloud uses federated authentication and user permission settings to ensure that HUAWEI CLOUD Stack and HUAWEI CLOUD account permissions are consistent. In this way, HUAWEI CLOUD Stack VDC users can directly access the HUAWEI CLOUD console and use HUAWEI CLOUD services. The federated cloud does not need to interconnect with HUAWEI CLOUD services one by one, which solves the problems faced by traditional hybrid cloud solutions. **SSO:** If customers need to log in to multiple systems, customers can configure SSO to implement the SSO function. After logging in to the server system, you can log in to other client systems without entering the user name and password repeatedly. **Alarm monitoring:** HUAWEI CLOUD provides the alarm monitoring function. O&M personnel can monitor and manage alarms or events reported by the system or managed objects. Alarm monitoring provides various

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
			monitoring and handling rules and notifies O&M personnel of faults. This helps O&M personnel efficiently monitor, quickly locate, and handle network faults, ensuring normal service running. Log management: HUAWEI CLOUD ManageOne provides log management, which consists of unified logs and O&M plane log management. It provides efficient and secure log collection, query, storage, download, configuration, and management functions, helping O&M personnel easily cope with O&M scenarios such as log collection and query.

No.	Control Domain	SPECIFIC CONTROL REQUIREMENTS	HUAWEI CLOUD RESPONSE
Art .25	General Provision	The presentation of type I and type II reports of the SOC 2 audit, proven compliance with cloud security standards, is an essential condition, both to enable participation in the bidding process, and to renew the cloud service delivery contract with organs or entities of the federal public administration.	HUAWEI has set up a dedicated security audit team to periodically review compliance with security laws and regulations worldwide as well as internal security requirements. The team dedicates over ten members to perform a two-month long annual audit on Huawei Cloud operations worldwide, paying close attention to such Huawei Cloud aspects as legal, regulatory, and procedural compliance; business goal and milestone accomplishment; integrity of decision-making information; and security O&M risks. Audit results are reported to HUAWEI' s Board of Directors and executive management, who ensure that any and all identified issues are properly resolved and closed. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications and is audited by third parties every year. HUAWEI CLOUD has completed the SOC audit project and adopted the five control attributes of SOC 2 Type 2. (Security, Availability, Process Integrity, Confidentiality, Privacy), which complies with cloud security standards. If necessary, government agencies can apply to HUAWEI CLOUD for a copy of the SOC2 audit report through official channels.

6 Conclusion

HUAWEI CLOUD is committed to providing government customers with a secure cloud environment that meets regulatory requirements and continuously improves HUAWEI CLOUD's security assurance system and security capabilities to improve compliance with government regulatory standards. This document describes HUAWEI CLOUD's security practices in key areas of government regulation. It helps customers in the government industry learn more about HUAWEI CLOUD's compliance with government regulation requirements and help customers use HUAWEI CLOUD safely and securely. In addition, this document provides guidance for customers on how to design, build, and deploy a secure cloud environment that meets government and industry regulatory requirements on HUAWEI CLOUD, helping customers better share security responsibilities 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 use of cloud services as appropriate and ensure compliance with government and industry regulatory requirements and other applicable laws when using HUAWEI CLOUD.

7 Version History

Date	Version	Description
2022-8	1.0	First release