White Paper for HUAWEI CLOUD Trustworthiness

Issue	1.1
Date	2024-08-14

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/

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to “Vul. Response Process”. For details about the policy, see the following website:

https://www.huawei.com/en/psirt/vul-response-process

For enterprise customers who need to obtain vulnerability information, visit:

https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview

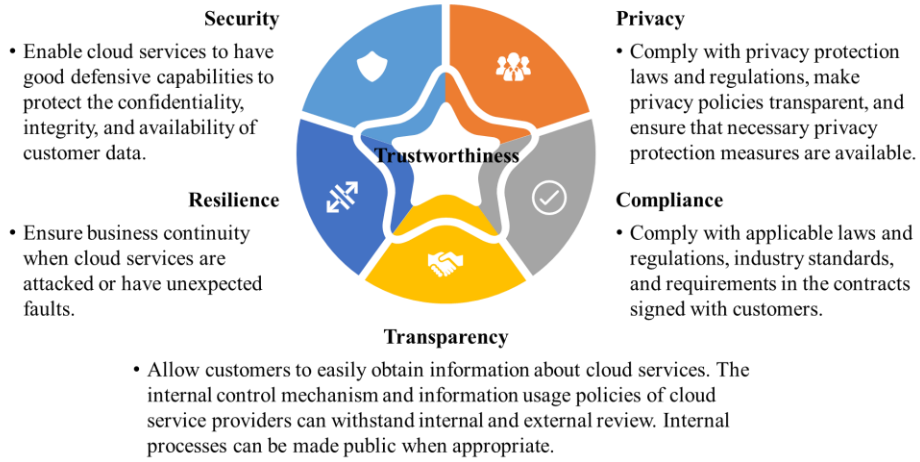
When cloud computing was still in its infancy, cloud was favored by small and micro enterprises, especially Internet enterprises, because of its quick scalability and low initial investment. Large and medium-sized enterprises also used the cloud, but as a supplement to their core business systems. At that time, customers' main requirements for cloud services were that they should implement functions quickly and deliver elastic scalability. As cloud computing functions become more diversified and complete, many enterprises are gradually migrating their core systems to the cloud. The cloud plays an important role in the digital transformation of enterprises, the upgrade of business models, and even the transformation of entire industries. When choosing cloud services, governments, enterprises, and individual users first consider how the cloud services implement lifecycle trustworthiness and provide trustworthy products and services.

Over the past 30 years, Huawei, one of the world's leading ICT service providers, has delivered advanced, stable, reliable, and secure products and services for industries, enterprises, and individuals in more than 170 countries and regions while adhering to continuous technical innovation and service promotion. HUAWEI CLOUD, established by Huawei as a strategic business, has inherited Huawei's strong internationalization attributes, ensuring it complies with applicable laws and regulations while also meeting the requirements of customers in numerous industries around the world to build trustworthy cloud services. By the end of June 2019, HUAWEI CLOUD, together with its partners, has opened 44 availability zones (AZs) in 23 locations worldwide. In strict compliance with industry standards and business boundaries, and following Huawei's customer-centricity and trustworthiness principles, HUAWEI CLOUD works with ecosystem partners to build superior and trustworthy cloud services.

Mr. Ren Zhengfei, founder and CEO of Huawei, said: "We are committed to building trust and high quality into every ICT infrastructure product and solution we develop... We will place trustworthiness above all else. Over function, feature, and product schedule," in a 2019 open letter to all employees, titled *Comprehensively Enhancing Software Engineering Capabilities and Practices to Build Trustworthy, Quality Products*.

Trustworthiness is the most important and fundamental requirement for cloud services and is a concept in which HUAWEI CLOUD firmly believes. Establishing and improving a trust mechanism for the services HUAWEI CLOUD provides is the top priority. After thoroughly analyzing the industry's interpretation of trustworthiness and listening carefully to customer feedback, HUAWEI CLOUD has determined that cloud service trustworthiness should include five essential features: **security, privacy, compliance, resilience, and transparency**.

Figure 1-1 Five essential features of HUAWEI CLOUD trustworthiness



Security

- Enable cloud services to have good defensive capabilities to protect the confidentiality, integrity, and availability of customer data.

Privacy

- Comply with privacy protection laws and regulations, make privacy policies transparent, and ensure that necessary privacy protection measures are available.

Resilience

- Ensure business continuity when cloud services are attacked or have unexpected faults.

Compliance

- Comply with applicable laws and regulations, industry standards, and requirements in the contracts signed with customers.

Transparency

- Allow customers to easily obtain information about cloud services. The internal control mechanism and information usage policies of cloud service providers can withstand internal and external review. Internal processes can be made public when appropriate.

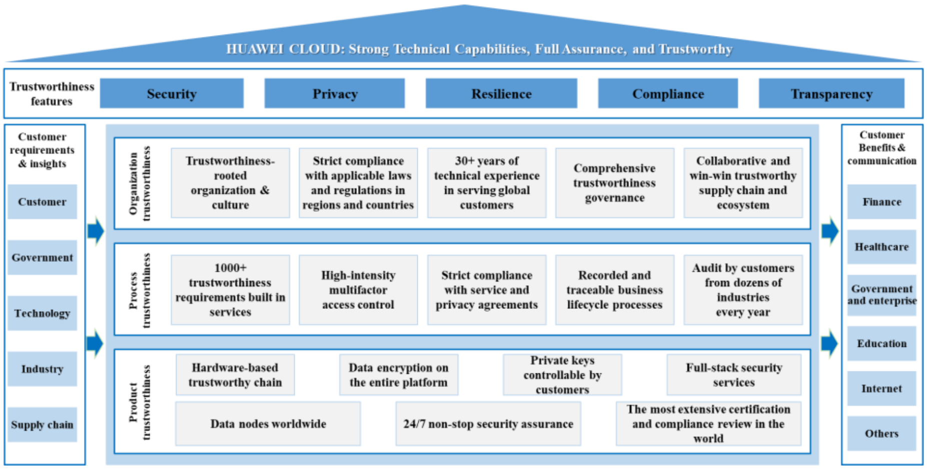
To create products that are truly trustworthy, Huawei believes it is essential that trustworthy organizations implement trustworthy processes. By building a top-down trustworthy organization, HUAWEI CLOUD improves the trustworthiness awareness and capabilities of all development, O&M, and operation personnel and applies personnel, regulations, and technologies to internal and external processes, enabling the continuous launch, update, and optimization of trustworthy products, solutions, and services. **Organization, process, and product** are three critical dimensions in which HUAWEI CLOUD fulfills trustworthiness requirements.

Trustworthy organization: Adhering to the principle of data neutrality, HUAWEI CLOUD has established a comprehensive, compliant, transparent, and stable internal control mechanism by building trustworthiness into the enterprise through the management system, from the enterprise strategy, organizational culture, and risk management, to the supply chain and ecosystem.

Trustworthy process: HUAWEI CLOUD establishes, implements, and maintains an end-to-end business process management system, covering product R&D, O&M, and customer service, and continuously improves the system to ensure that processes are rigorous, complete, and traceable.

Trustworthy product: HUAWEI CLOUD's entire portfolio of cloud services are provided based on trusted cloud infrastructure and products to meet customer requirements and quickly adapt to internal and external environment and business changes.

Figure 1-2 HUAWEI CLOUD trustworthiness framework


HUAWEI CLOUD: Strong Technical Capabilities, Full Assurance, and Trustworthy
Trustworthiness features
Security
Privacy
Resilience
Compliance
Transparency
Customer requirements & insights
Customer
Government
Technology
Industry
Supply chain
Organization trustworthiness
Trustworthiness-rooted organization & culture
Strict compliance with applicable laws and regulations in regions and countries
30+ years of technical experience in serving global customers
Comprehensive trustworthiness governance
Collaborative and win-win trustworthy supply chain and ecosystem
Process trustworthiness
1000+ trustworthiness requirements built in services
High-intensity multifactor access control
Strict compliance with service and privacy agreements
Recorded and traceable business lifecycle processes
Audit by customers from dozens of industries every year
Product trustworthiness
Hardware-based trustworthy chain
Data encryption on the entire platform
Private keys controllable by customers
Full-stack security services
Data nodes worldwide
24/7 non-stop security assurance
The most extensive certification and compliance review in the world
Customer Benefits & communication
Finance
Healthcare
Government and enterprise
Education
Internet
Others

This white paper describes how HUAWEI CLOUD implements five trustworthiness features (security, privacy, resilience, compliance, and transparency) from three dimensions (trustworthy organization, process, and product), demonstrating HUAWEI CLOUD's determination and capabilities to build trustworthiness for customers, partners, and other stakeholders, connect developers and industry partners, and enable customers to jointly build a trustworthy ecosystem.

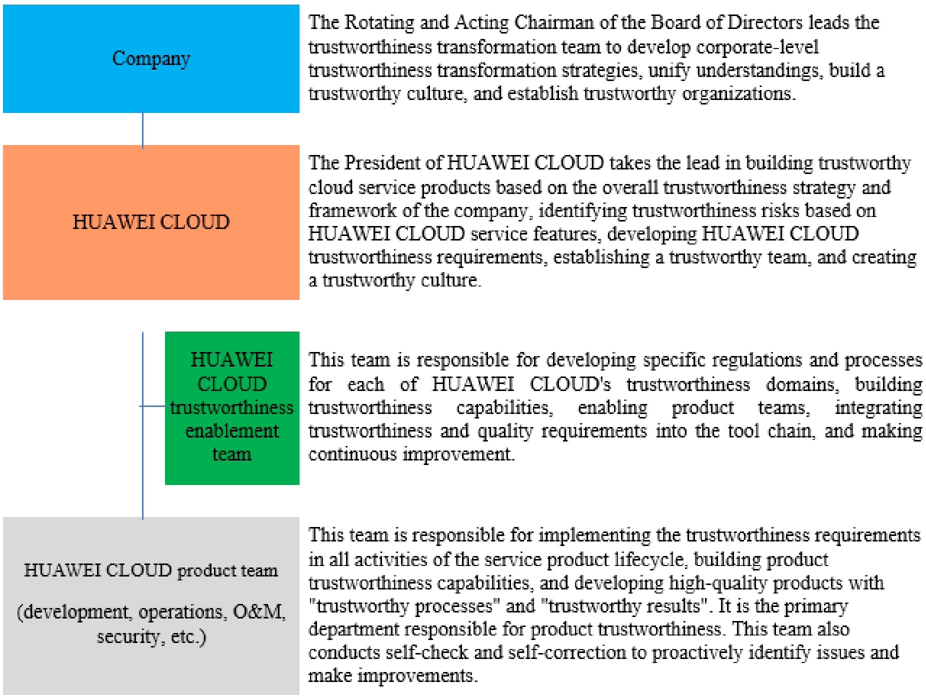
2 Trustworthy Organization – Trustworthy Organization, Culture, and Governance

Trustworthiness applies to not only products and systems, but also the organization, culture, and governance. HUAWEI CLOUD firmly believes in this concept and deeply integrates trustworthiness into its organizational culture, which is risk-driven. Through comprehensive trustworthiness governance, HUAWEI CLOUD meets the requirements of applicable laws and regulations, certification processes, and audits worldwide, and transfers trustworthiness capabilities to the supply chain and industry ecosystem to ensure that trustworthy products and services can be continuously produced.

2.1 Trustworthiness-rooted Organization and Culture

It is essential that trustworthiness be built into the enterprise. At both the company and HUAWEI CLOUD levels, trustworthiness enablement centers and management organizations are set up with the following main functions:

Figure 2-1 Trustworthy organization of HUAWEI CLOUD


Company
HUAWEI CLOUD
HUAWEI CLOUD trustworthiness enablement team
HUAWEI CLOUD product team
(development, operations, O&M, security, etc.)

The Rotating and Acting Chairman of the Board of Directors leads the trustworthiness transformation team to develop corporate-level trustworthiness transformation strategies, unify understandings, build a trustworthy culture, and establish trustworthy organizations.

The President of HUAWEI CLOUD takes the lead in building trustworthy cloud service products based on the overall trustworthiness strategy and framework of the company, identifying trustworthiness risks based on HUAWEI CLOUD service features, developing HUAWEI CLOUD trustworthiness requirements, establishing a trustworthy team, and creating a trustworthy culture.

This team is responsible for developing specific regulations and processes for each of HUAWEI CLOUD's trustworthiness domains, building trustworthiness capabilities, enabling product teams, integrating trustworthiness and quality requirements into the tool chain, and making continuous improvement.

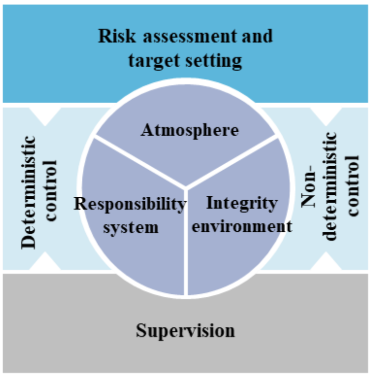
This team is responsible for implementing the trustworthiness requirements in all activities of the service product lifecycle, building product trustworthiness capabilities, and developing high-quality products with "trustworthy processes" and "trustworthy results". It is the primary department responsible for product trustworthiness. This team also conducts self-check and self-correction to proactively identify issues and make improvements.

Guided by the trustworthiness strategy and framework, departments at all levels of the company and HUAWEI CLOUD are committed to building a trustworthy culture, ensuring all employees understand trustworthiness, and building trustworthiness into all aspects of the company. We have also established management requirements for software engineering trustworthiness and competency. These requirements allow us to better select and regulate software business directors, committers, software architects, development engineers, and test engineers in addition to managing their qualifications. In addition, to ensure that software engineers are capable of writing trustworthy high-quality code for products, they are required to learn the trustworthiness requirements and pass the corresponding exams.

2.2 Comprehensive Trustworthiness Governance

HUAWEI CLOUD trustworthiness governance complies with the corporate Risk Governance Control (RGC) framework. Driven by risks, HUAWEI CLOUD establishes the integrity environment and atmosphere by specifying the risk responsibility system, develops and implements control measures, and continuously monitors and ensures effective risk control.

Figure 2-2 Trustworthiness governance methodology framework of HUAWEI CLOUD



7 elements

- **Risk assessment and target setting**
- **Atmosphere**
- **Responsibility system**
- **Integrity environment**
- **Deterministic control**
- **Non-deterministic control**
- **Supervision**

Guided by the RGC framework, HUAWEI CLOUD implements all-round and multi-dimensional risk management in terms of data security, privacy protection, compliance, and operation, and minimizes the risks of HUAWEI CLOUD services to an acceptable level.

To handle security and privacy risks, HUAWEI CLOUD has established an information security management system (ISMS) and a privacy information management system (PIMS) in accordance with international standards. These systems enable us to systematically carry out information security risk assessment and privacy impact assessment (PIA), fully identify and analyze security and privacy risks, and develop and implement mitigation measures. We are committed to customer data security and privacy protection.

To handle compliance risks, HUAWEI CLOUD strictly complies with all applicable laws and regulations in the countries where we operate, systematically identifies and manages compliance risks, and develops contingency plans. We also carry out training and drills to improve the organizational compliance awareness and our emergency-handling capabilities. We believe that compliance with global laws and regulations is the foundation for Huawei's survival, service, and contribution worldwide.

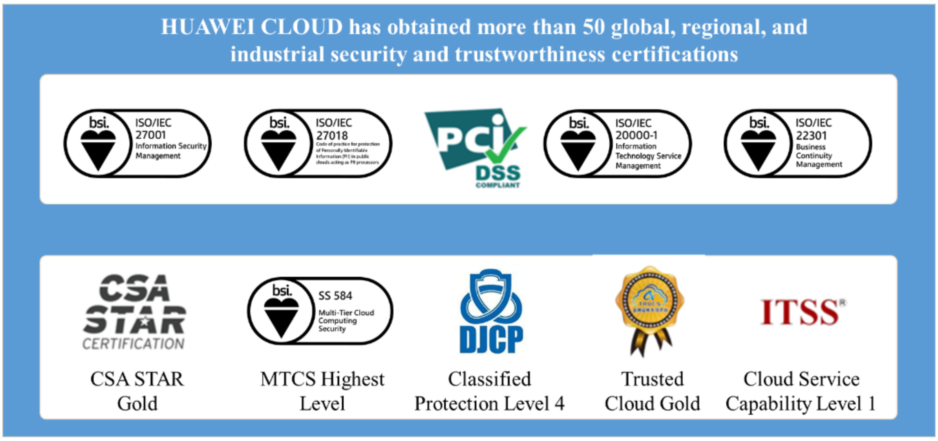
To handle business continuity risks, we have established an end-to-end continuous business improvement and optimization management mechanism from suppliers to HUAWEI CLOUD and from HUAWEI CLOUD to customers. We have also carried out business impact analysis and risk assessment by establishing policies, organizations, regulations, processes, baselines, and IT platforms to improve the compliance of our organizations with relevant corporate regulations and processes. In addition, we implement effective management of daily business risks, ensure the business continuity of HUAWEI CLOUD organizations and cloud services, and effectively support the stable operation of customer systems and businesses.

2.3 Strict Compliance, Certification, and Audit Assurance

Compliance is the basis for security and trustworthiness. HUAWEI CLOUD leverages Huawei's global industrial layout and in-depth understanding of the different cultures and laws around the world. In accordance with applicable laws and regulations, industry standards, customer requirements, and industry best-practices, we endeavor to ensure compliance and support customer compliance.

Numerous certification organizations, authoritative in their respective fields, have independently assessed and reviewed HUAWEI CLOUD in terms of personnel management, resources, technologies, and processes. They all conclude that HUAWEI CLOUD meets strict standards in terms of security and trustworthiness.

Figure 2-3 Certifications and assessments of HUAWEI CLOUD


HUAWEI CLOUD has obtained more than 50 global, regional, and industrial security and trustworthiness certifications
bsi. ISO/IEC 27001 Information Security Management
bsi. ISO/IEC 27018 Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
PCI DSS COMPLIANT
bsi. ISO/IEC 20000-1 Information Technology Service Management
bsi. ISO/IEC 22301 Business Continuity Management
CSA STAR CERTIFICATION
CSA STAR Gold
bsi. SS 584 Multi-Tier Cloud Computing Security
MTCS Highest Level
DJCP
Classified Protection Level 4
Trusted Cloud Gold
ITSS®
Cloud Service Capability Level 1

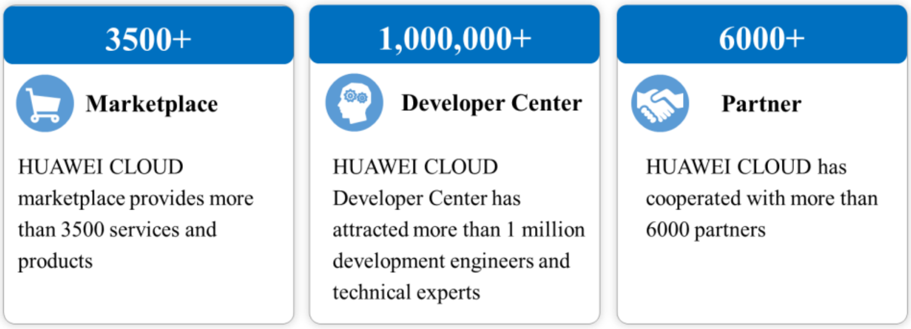
HUAWEI CLOUD actively invites customers and third-party auditors to participate in our security and trustworthiness audits and observe our remarkable growth in security and trustworthiness. We are also proactive in joining various international standards organizations, industry alliances, and open source communities. In addition, we open our trustworthiness capabilities free of charge to third-party organizations, contributing to the healthy development of the entire ICT industry.

2.4 Collaborative and Win-Win Trustworthy Supply Chain and Ecosystem

Cloud computing is a complex combination of IT software, hardware, and services, and involves a wide range of basic components provided by numerous different suppliers. A secure and trustworthy supply chain is important for trustworthy cloud service products. For enterprises that provide basic components on the supply chain, HUAWEI CLOUD ensures that products and services meet security and trustworthiness requirements through strict supplier sourcing processes and performance appraisal measures.

With an open and win-win attitude, HUAWEI CLOUD works with suppliers, developers, and partners to build a user-centric cloud service ecosystem. In addition to Huawei-developed cloud products, customers can select third-party cloud products that are strictly vetted by HUAWEI CLOUD from the cloud marketplace. Developers can use the HUAWEI CLOUD developer center to efficiently and conveniently develop trustworthy cloud products that meet their own requirements.

Figure 2-4 Cooperation and supply ecosystem of HUAWEI CLOUD



3500+

Marketplace

HUAWEI CLOUD marketplace provides more than 3500 services and products

1,000,000+

Developer Center

HUAWEI CLOUD Developer Center has attracted more than 1 million development engineers and technical experts

6000+

Partner

HUAWEI CLOUD has cooperated with more than 6000 partners

To ensure that all cloud products in the cloud marketplace are high quality and reliable, HUAWEI CLOUD follows the principle of "selecting the best of the best" and formulates unified rules. Before vendors, partners, and products can enter the cloud marketplace, they must pass our strict threshold qualifications. This helps control the software and application service providers in terms of scale and qualification, security and trustworthiness capabilities, and technical R&D strength from the source. It also ensures that users obtain only high-quality products from the cloud marketplace. In addition, HUAWEI CLOUD uses supervision and punishment mechanisms for registered vendors and partners (specified in service agreements). If any registered vendors, partners, or their cloud products fail to meet their obligations to customers, HUAWEI CLOUD requires them to bear all liabilities.

The HUAWEI CLOUD developer center provides a development environment, OpenAPI, software development kits (SDKs), and lifecycle-based one-stop application development services, making software development simpler and more efficient. The developer center also provides tools such as code check, test management, source code control, and issue and bug tracing tools to help developers create secure and trustworthy products.

HUAWEI CLOUD aims to deliver the best experience to customers, provide neutral cloud infrastructure that is stable, reliable, secure, trustworthy, sustainable, and innovative, and converge the ecosystem on the cloud infrastructure to resolve problems customers have during digital transformation.

3 Process Trustworthiness — Trustworthy Process Management Throughout the Entire Lifecycle

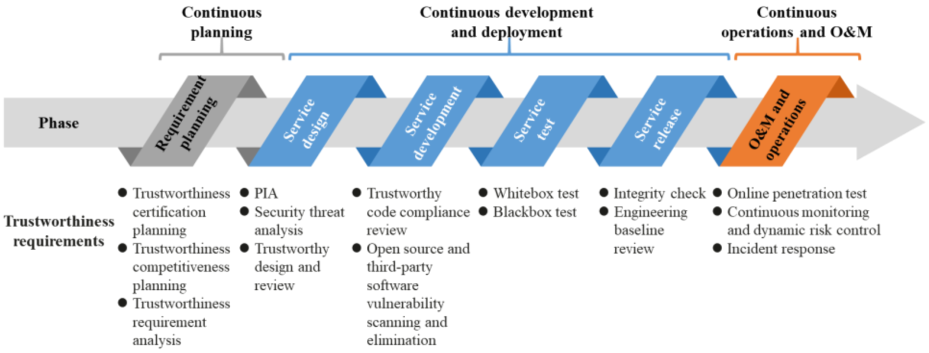
Huawei has always advocated a corporate culture of delivering secure and trustworthy software products. This is also at the heart of HUAWEI CLOUD, where we believe that the trustworthiness of cloud services should be reflected in not only technologies and products, but also the entire lifecycle, which includes requirement planning, architecture design, system development, O&M, operations, and customer services. Regardless of internal business processes or external customer services, HUAWEI CLOUD fully complies with the basic principles of security, compliance, and privacy protection required by laws, regulations, and international standards. We have formulated more than 1000 trustworthiness requirements to incorporate function, quality, security, and privacy protection requirements into the full lifecycle of cloud services, focusing on privacy protection during the collection, use, retention, transfer, disclosure, and disposal of personal information. This ensures that the processes are transparent, well-structured, strictly controlled, and traceable.

3.1 Development and O&M Processes with Built-in Trustworthiness

Over the past two decades, the IPD process has helped Huawei significantly improve the quality of ICT products. Today, to meet the requirements of quick service delivery in the cloud environment, HUAWEI CLOUD continuously improves the development and O&M processes based on industry-leading concepts and employs DevSecOps, a trustworthy software engineering process that integrates development, O&M, and security.

HUAWEI CLOUD DevSecOps achieves process standardization through tools and technical specifications, makes processes and results transparent, and enables tracing from fault symptoms to module code, ensuring process trustworthiness throughout the entire lifecycle of cloud services.

Figure 3-1 HUAWEI CLOUD DevSecOps lifecycle model


Continuous planning
Continuous development and deployment
Continuous operations and O&M
Phase
Requirement planning
Service design
Service development
Service test
Service release
O&M and operations
Trustworthiness requirements
● Trustworthiness certification planning
● Trustworthiness competitiveness planning
● Trustworthiness requirement analysis
● PIA
● Security threat analysis
● Trustworthy design and review
● Trustworthy code compliance review
● Open source and third-party software vulnerability scanning and elimination
● Whitebox test
● Blackbox test
● Integrity check
● Engineering baseline review
● Online penetration test
● Continuous monitoring and dynamic risk control
● Incident response

The DevSecOps process focuses on two key indicators, namely, quality and efficiency, to implement process trustworthiness. This process embodies the following concepts:

- Trustworthiness is the responsibility of all team members. Achieving trustworthiness is central to the way each Huawei employee thinks and works.
- Trustworthiness starts from R&D planning and requirement review. Building trustworthiness is the basis of the design process to achieve security & privacy by design and by default.
- Security and quality assurance measures are seamlessly integrated into the entire lifecycle of DevSecOps and can be automatically implemented.
- DevSecOps strengthens the feedback and continuous improvement mechanisms, establishes small cycles between modules, drives service product innovation through O&M and operations, and continuously launches cloud services that lead the industry development.
- Technical architecture decoupling is the basis of the DevSecOps pipeline. Cloud software products can be independently developed, tested, released, deployed, and maintained.

HUAWEI CLOUD launches commercial DevCloud software development products that adhere to internal DevSecOps practices. In addition to providing services externally, DevCloud is a continuous integration and delivery platform used by the HUAWEI CLOUD R&D and O&M teams. It integrates specifications, baselines, software/APIs, cases, and tools into the DevSecOps pipeline, forming an automated and visualized process for service lifecycle management.

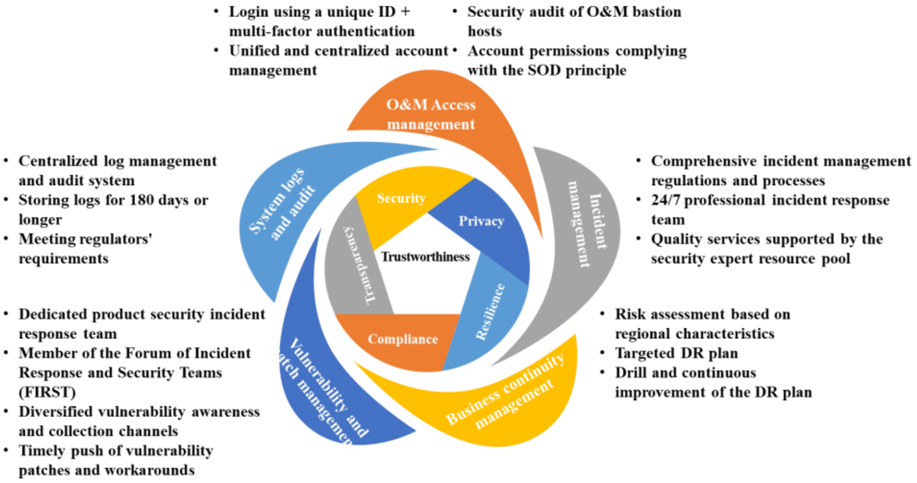
3.2 Secure, Stable, and Trustworthy Operations

To ensure secure and stable running of cloud services, HUAWEI CLOUD has established a trustworthy operations center that provides O&M permission management, system log and audit, vulnerability and patch management, event management, business continuity management, and other O&M and operations services. This operations center covers the entire lifecycle of security operations, including pre-event prevention, in-event response, and post-event audit. HUAWEI CLOUD has also determined the trustworthiness requirements in terms of compliance, transparency, privacy protection, and other aspects and incorporated them into cloud service operations activities. Taking monitoring and log management as an example:

- Logs can be stored for more than 180 days, meeting regulatory compliance requirements

- Logs do not contain users' sensitive personal information, meeting privacy requirements
- Notifications of vulnerabilities and events are pushed in a timely manner, meeting transparency requirements
- Users are free to choose the notification push means, meeting privacy requirements

Figure 3-2 Trustworthy operations of HUAWEI CLOUD



- Login using a unique ID + multi-factor authentication
- Unified and centralized account management
- Security audit of O&M bastion hosts
- Account permissions complying with the SOD principle

- Comprehensive incident management regulations and processes
- 24/7 professional incident response team
- Quality services supported by the security expert resource pool

- Risk assessment based on regional characteristics
- Targeted DR plan
- Drill and continuous improvement of the DR plan

- Dedicated product security incident response team
- Member of the Forum of Incident Response and Security Teams (FIRST)
- Diversified vulnerability awareness and collection channels
- Timely push of vulnerability patches and workarounds

- Centralized log management and audit system
- Storing logs for 180 days or longer
- Meeting regulators' requirements

3.3 High-Quality Customer Service

Customer service is a portal through which cloud service providers can communicate with customers. High-quality services also reflect trustworthiness. In order to build trust, HUAWEI CLOUD believes that creating a transparent and complete customer service mechanism is equally important as developing complete and trustworthy internal control processes.

HUAWEI CLOUD has established a complete and transparent customer service system, which we use in good faith to establish contact with customers, collect customers' requirements, resolve customers' issues, and improve the trustworthiness capabilities of products and services.

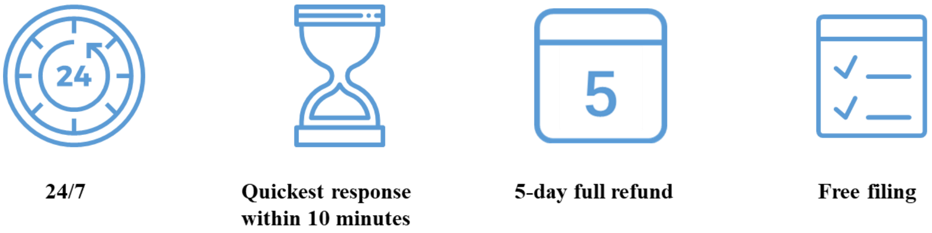
Service Agreement and Privacy Agreement

HUAWEI CLOUD has released *HUAWEI CLOUD User Agreement*, *Cloud Service Level Agreement (SLA)*, and *Privacy Policy Statement* on its official website, providing clear and transparent information and helping customers understand HUAWEI CLOUD responsibilities, product service indicators, and privacy protection information. HUAWEI CLOUD provides multiple interactive channels for customers to acquire and execute data subjects' rights.

Customer Service and Support Plan

As a customer- and service-oriented business, HUAWEI CLOUD provides different levels of service packages (basic, developer, business, and enterprise levels). Users can obtain professional services and support through the online ticket system, intelligent customer service, self-service, and hotline.

Figure 3-3 HUAWEI CLOUD service and support



Service request and customer authorization

When handling service requests, HUAWEI CLOUD obtains the customer's authorization for all activities related to customer network operations in advance, and performs operations in strict accordance with the authorization scope, period, and usage to ensure that the authorization and operation records are traceable. We also use technical means such as access control, encryption, and anonymization to effectively protect customers' privacy data.

Feedback and Suggestion Channels

Any user can access services, provide feedback, and make complaints and suggestions through multiple channels. In addition to the online customer service and the complaint and suggestion hotline, enterprise customers with complex systems can choose appropriate support plans to obtain dedicated support from IM enterprise groups, technical account managers (TAMs), and service managers.

HUAWEI CLOUD support and service website: https://support-intl.huaweicloud.com/en-us/help-tools.html

4 Product Trustworthiness – Trustworthy Cloud Infrastructure and Services

The security of cloud services depends on both cloud service providers and customers. HUAWEI CLOUD is responsible for establishing and managing physical infrastructure and providing basic and application services. Customers are responsible for the secure configuration and management of the cloud services they purchase and use. Based on the in-depth defense and default isolation principles, HUAWEI CLOUD deploys high-level IT infrastructure globally to ensure the security of basic services of networks, platforms, and APIs and implement security protection for data and applications throughout their lifecycles.

4.1 High-Level, Highly Available, and Global IT Infrastructure

High-Level Data Center (DC) Equipment Room

Leveraging years of experience in constructing telecommunications equipment rooms, HUAWEI CLOUD employs stringent standards when selecting and building cloud DCs. We fully consider both natural and human factors when selecting sites, and ensure that each availability zone (AZ) is physically isolated and independently maintained. Our construction of equipment rooms complies with the T3 standard in TIA 942 *Telecommunications Infrastructure Standard for Data Centers*.

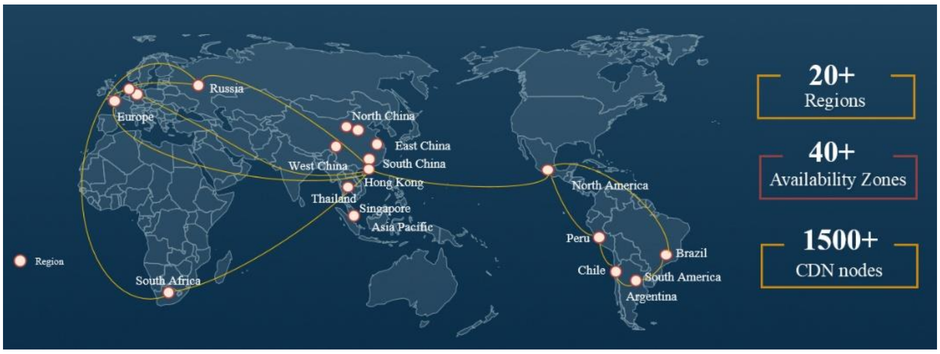
Highly Available DC Architecture

HUAWEI CLOUD deploys multiple AZs in each region, and multiple DCs in each AZ. DCs in each region or AZ are interconnected through high-speed optical fibers. We use data replication and all-active technologies to prevent the loss of data and ensure service continuity in AZs.

Global Infrastructure

As a world-leading ICT product and solution provider, Huawei has deployed cloud platforms for more than 270 carriers and their regions worldwide. These platforms use cloud computing solutions with the unified architecture of private cloud, public cloud, and hybrid cloud. In the public cloud field, HUAWEI CLOUD has established and deployed dozens of regions across five continents.

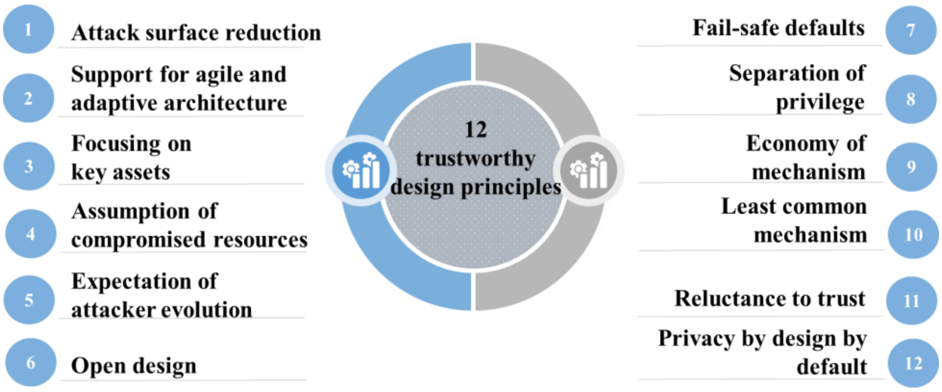
Figure 4-1 HUAWEI CLOUD global IT infrastructure



4.2 Comprehensive Basic Service Security Assurance

By leveraging Huawei's years of product development experience, listening to customer requirements, and following industry standards, HUAWEI CLOUD has formulated 12 trustworthy design principles for cloud services.

Figure 4-2 12 trustworthy design principles for HUAWEI CLOUD


1 Attack surface reduction
2 Support for agile and adaptive architecture
3 Focusing on key assets
4 Assumption of compromised resources
5 Expectation of attacker evolution
6 Open design
12 trustworthy design principles
Fail-safe defaults 7
Separation of privilege 8
Economy of mechanism 9
Least common mechanism 10
Reluctance to trust 11
Privacy by design by default 12

HUAWEI CLOUD uses multiple technical means to apply design principles to full-stack cloud service R&D and implementation, covering the entire lifecycle from product design to product implementation. We also use multiple protection layers, including basic network protection, platform isolation, and application security. This enables us to achieve comprehensive security assurance for basic services.

Basic Cyber Security

To enhance cyber security protection and contain cyber attacks, HUAWEI CLOUD employs ITU E.408 security zone division principles and industry-leading cyber security practices to divide and isolate the security zones and network planes of the HUAWEI CLOUD network. In addition, we use technical means to clean up abnormal and super-large DDoS traffic, detect and prevent network intrusions (using IDS/IPS), and protect web security.

Platform Isolation

HUAWEI CLOUD uses a unified virtualization platform (UVP) to virtualize physical server resources, such as CPU, memory, and I/O resources, into a group of logical resources. These resources can then be centrally managed, flexibly scheduled, and dynamically allocated. They create an environment on a single physical server for multiple isolated virtual machines (VMs) to run simultaneously. In China's Trusted Cloud Services (TRUCS) certification, cloud hosts of the HUAWEI CLOUD platform obtain the highest level of Five Star+ Certification.

The virtual private cloud (VPC) product offered by HUAWEI CLOUD is the key to network isolation. With the VPC, tenants can control their own virtual networks, implementing Layer 2 and Layer 3 network isolation between tenants. The security group function of the VPC allows users to configure security and access rules as required, meeting tenants' requirements for fine-grained network isolation.

Application Security

HUAWEI CLOUD services can be configured and managed through open APIs to interconnect with the existing IT management and audit systems of enterprises. As a critical security boundary for services, APIs are protected using multiple mechanisms and measures:

- HUAWEI CLOUD performs identity authentication on each API request through the integrated Identity and Access Management (IAM) system. The transmission channel is encrypted using Transport Layer Security (TLS).
- Each access request is authenticated based on the token or access key ID/secret access key.
- Multiple advanced boundary protection mechanisms, such as anti-DDoS, IPS, and web application firewall (WAF), are used to defend against various threats and attacks.
- On the basis of advanced boundary protection, only registered APIs can be accessed by tenants, ACL rules are configured to allow only specified tenants and network segments to access the API gateway, and API traffic is controlled for highly available and continuous API-based access.

4.3 Data Security Throughout the Entire Lifecycle

Data Creation

HUAWEI CLOUD provides services by region. A region is the location where a customer stores content data. Without authorization, HUAWEI CLOUD will not move a customer's content data across regions. Access control mechanisms of different granularities ensure that customers can access only their own data.

Data Storage

HUAWEI CLOUD provides data encryption and storage protection on the cloud by using the dedicated hardware security module (DHSM), key management system (KMS), and key pair management functions of the data encryption workshop (DEW).

DHSM is a hardware encryptor that complies with the Office of the State Commercial Cryptography Administration (OSCCA) certification or FIPS 140-2 level-3 certification. It provides up to 10,000 TPS user-exclusive encryption capabilities. KMS provides encryption features and secure key management for cloud services. Customers can use KMS to manage keys securely. KMS keys are protected by the hardware security module (HSM), which has obtained FIPS 140-2 security certification (level 2 and level 3), meeting data compliance requirements.

Data Transmission

HUAWEI CLOUD uses virtual private networks (VPNs) to establish secure encrypted communication tunnels between remote users and VPCs, seamlessly extending existing data centers to HUAWEI CLOUD and ensuring end-to-end data transmission confidentiality for tenants. Through the communication tunnels established using VPNs between traditional data centers and VPCs, customers can conveniently use HUAWEI CLOUD resources.

HUAWEI CLOUD services are released in the standard RESTful format. Data transmitted over the entire network is encrypted using TLS. In addition, HUAWEI CLOUD services support target website identity authentication based on the X.509 certificate.

Data Backup and Restoration

HUAWEI CLOUD provides multiple redundancy and disaster recovery mechanisms to ensure high data durability and service availability. The availability of many products matches the highest levels in the industry.

Table 4-1 Data durability and availability assurance indicators of HUAWEI CLOUD

Storage Type	Service Availability/Data Durability
Elastic Volume Service (EVS)	Data durability: 99.9999999%
Volume Backup Service (VBS)	Data durability: 99.999999999%
Object Storage Service (OBS)	Data durability: 99.9999999999%; service availability: 99.995%
Relational Database Service (RDS)	Hot backup architecture, backup files retained for 732 days, automatic switchover within 1 minute
Image Management Service (IMS)	Private image redundancy by storing multiple copies; data durability up to 99.999999999%.

Data Deletion and Destruction

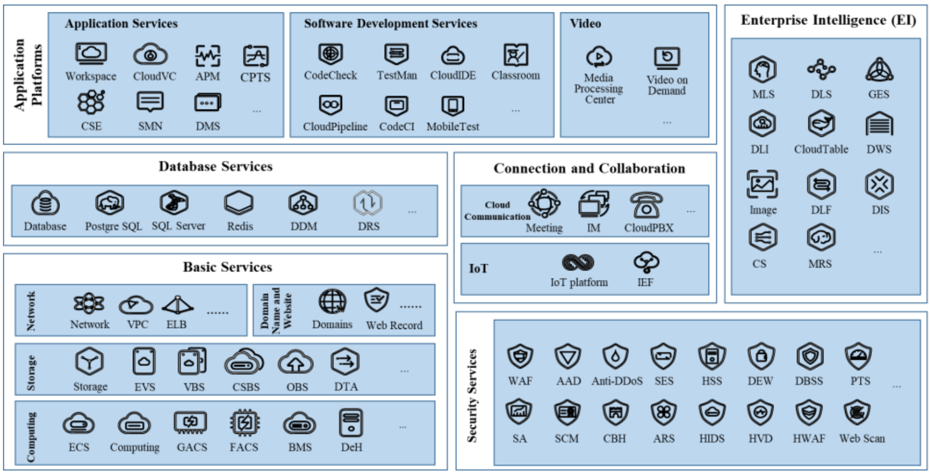
After a user confirms data deletion, HUAWEI CLOUD securely deletes the user data and all copies of it by means of memory clearance, logical deletion, virtual volume deletion, and encryption key destruction. After a user deregisters a HUAWEI CLOUD account, the associated content data enters the retention period. During this period, the user cannot access or use cloud services. After the retention period expires, the content data is permanently deleted. When physical storage media need to be decommissioned, HUAWEI CLOUD permanently deletes the data in the storage media by means of degaussing, bending, or shredding to prevent the data from being restored.

5 Trustworthiness Enablement – HUAWEI CLOUD Helps Customers Achieve More Trustworthy Services

HUAWEI CLOUD ensures the trustworthiness of its products and releases accumulated trustworthiness capabilities through full-stack services and solutions to help customers achieve trustworthiness in terms of security, privacy, resilience, compliance, and transparency.

HUAWEI CLOUD provides more than 100 types of secure, reliable, and stable services in six categories and continuously enriches and optimizes the services based on industry development and customer requirements. The following figure shows the full-stack service classification and products of HUAWEI CLOUD.

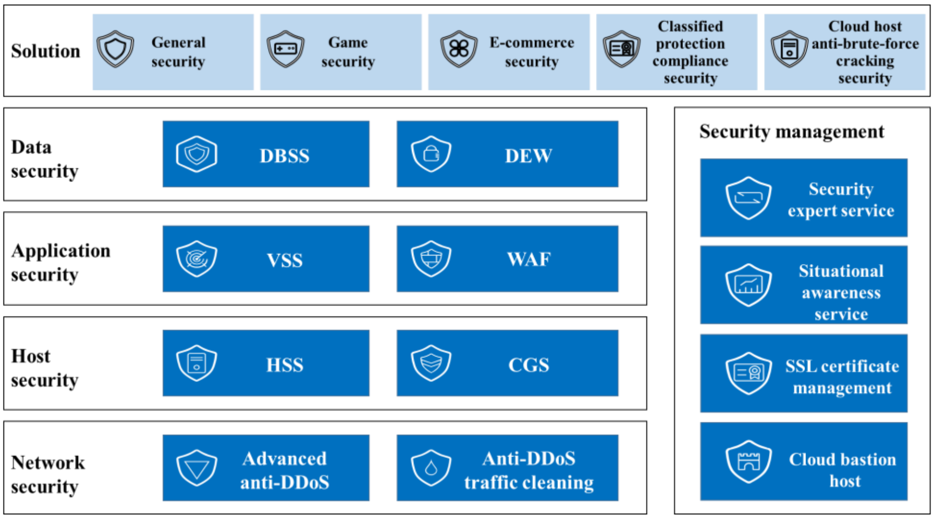
Figure 5-1 Full-stack service classification and products of HUAWEI CLOUD



Security Enablement

To meet the security requirements of various types of customers, covering individual users and multinational enterprises, HUAWEI CLOUD designs and develops security products and solutions that are easy to use and provide comprehensive functions. HUAWEI CLOUD provides full-stack security services based on attack patterns and paths of different levels. In addition, HUAWEI CLOUD provides security solutions based on typical security risks and service architecture characteristics of industries such as gaming, e-commerce, and finance, helping customers ensure service security.

Figure 5-2 HUAWEI CLOUD full-stack security services



The HUAWEI CLOUD WAF leverages Huawei's years of experience in attack and defense to intelligently identify malicious request features and defend against unknown threats through in-depth machine learning. It can detect and protect service traffic on customer websites from multiple dimensions, preventing common attacks such as Structured Query Language (SQL) injection and cross-site scripting (XSS). This helps prevent such attacks from affecting customers' web applications and reduce the risks of customer data being tampered with or stolen.

HUAWEI CLOUD's Host Security Service (HSS) improves the overall host security. It provides functions such as account cracking prevention, detection of weak passwords and malicious programs, two-factor authentication, vulnerability management, and web page anti-tampering, helping customers build a server security protection system and reduce major security risks faced by hosts.

Additionally, HUAWEI CLOUD works with third-party authorities to provide customers with expert services, assisting customers in preventing, monitoring, and detecting security risks of hosts and systems and repairing compromised systems in a timely manner.

Privacy Enablement

HUAWEI CLOUD integrates extensive privacy protection practices and R&D achievements into its cloud services. This provides customers with services capable of privacy protection, helps customers comply with privacy protection principles and requirements in their products and services, protects data subjects' rights, and quickly builds privacy compliance capabilities.

Identifying personal data, especially sensitive personal data, from systems is an important part of privacy protection. Customers can use the Database Security Service (DBSS) to automatically identify sensitive personal data such as ID card numbers and credit card numbers in the database based on the built-in compliance knowledge base or user-defined detection rules. Customers can customize protection policies for sensitive personal data. For example, they can use DEW to encrypt sensitive personal data to meet compliance requirements.

The Convergent Video Cloud Service (CVCS) provides interfaces for signing and querying privacy statements. This enables customers to easily embed the consent to privacy statements, or withdrawal of consent, in their products and services and record related operations, meeting privacy protection laws and regulations.

In scenarios such as online taxi hailing, express delivery, and real-estate agent, customers can use HUAWEI CLOUD's PrivateNumber service to provide private numbers for users without adding SIM cards. In this way, users can obtain high-quality call and SMS services while hiding their real numbers, protecting user privacy.

Resilience Enablement

Ensuring business continuity is a major challenge for every customer. HUAWEI CLOUD provides services and solutions for different risks to help customers reduce the impact of attacks, disasters, or faults.

In scenarios such as virus intrusion, manual deletion by mistake, and hardware and software faults, HUAWEI CLOUD provides the Cloud Backup and Recovery (CBR) service to restore data on the cloud servers and EVSs to any backup point.

To prevent unavailability of Internet services due to heavy-traffic DDoS attacks, customers can use the advanced anti-DDoS service provided by HUAWEI CLOUD for service stability and reliability.

To prevent fire and natural disasters from affecting services, HUAWEI CLOUD provides a cross-AZ, cross-region, and cloud-based geo-redundant disaster recovery (DR) solution to meet customers' DR requirements of different levels. In addition, HUAWEI CLOUD provides customers with professional cloud DR implementation services, helping customers design and implement DR solutions, perform DR drills, and provide training.

Compliance Enablement

HUAWEI CLOUD has obtained more than 50 global, regional, and industrial security and trustworthiness certifications. Because HUAWEI CLOUD infrastructure and services have already met a wide range of compliance requirements, customers need only pay attention to the compliance of their own applications.

Leveraging its security capabilities and security compliance ecosystem, HUAWEI CLOUD aggregates high-quality industry resources to provide one-stop compliance solutions for customers. This helps customers meet compliance requirements quickly and cost effectively. In addition, HUAWEI CLOUD seeks to further strengthen its cooperation with industry-recognized consulting companies and certification organizations to provide customers with more compliance certification solutions that meet their compliance requirements.

Transparency Enablement

To meet internal and external audit and inspection requirements and clearly understand the service running status, customers can use the log audit and monitoring service for backtracking to learn the resource usage and service running status on the cloud.

All HUAWEI CLOUD services provide basic logging. Customers can configure logging using the embedded function of each cloud service. They can also use the Log Tank Service (LTS) and Cloud Trace Service (CTS) to obtain centralized and complete logging and audit services.

The Cloud Eye Service (CES) enables customers to monitor resources such as elastic cloud servers and bandwidth resources in a multi-dimensional manner, comprehensively learn about resource usage and service running status on HUAWEI CLOUD, receive alarms, configure diversified notification modes and personalized report views, and accurately determine service resource status.

6 Closing Thoughts

HUAWEI CLOUD believes that trust is the foundation for any cooperation. Despite the rapid changes in business environments, technologies, and even the world in which we live, HUAWEI CLOUD will always regard trustworthiness as the first attribute. We work with global customers and partners to face challenges and build an open, cooperative, and win-win ICT ecosystem.

HUAWEI CLOUD: Strong Technical Capabilities, Full Assurance, and Trustworthy

For more information, visit:

HUAWEI CLOUD Trust Center:https://www.huaweicloud.com/intl/en-us/securecenter/overallsafety.html

HUAWEI CLOUD Security White Paper: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/SecurityWhitepaper_intl_en.pdf

White Paper for HUAWEI CLOUD Data Security:https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/DataSecurityWhitepaper_intl_en.pdf

White Paper for HUAWEI CLOUD Privacy Protection:https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/Privacy_Protection_intl_en.pdf