HUAWEI CLOUD Practice Guide for PCI DSS

Issue 3.0

Date 2023-02-07

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Overview

1.1 Scope of Application

The information provided in this document is applicable to the products and services provided by HUAWEI CLOUD on the official website.

1.2 Release Purpose and Target Audience

The Payment Card Industry Data Security Standard (PCI DSS) is an internationally recognized data security standard dedicated to protect cardholder data security. HUAWEI CLOUD has passed the PCI DSS certification, and wish to introduce to its customers the main controls implemented to ensure data security according to the standard requirements. This document is consequently intended for both customers who want to include HUAWEI CLOUD's environment within their PCI DSS evaluation during the certification process, as well as customers willing to learn more about HUAWEI CLOUD's data security policy by understanding:

- How HUAWEI CLOUD protects data security based on PCI DSS' requirements;
- HUAWEI CLOUD offers multiple products and services to customers to help them respond with PCI DSS.

1.3 Prerequisites

The versions of PCI DSS and official related guidelines mentioned in this document are identified in the section 6. This document does not contain all specific requirements of PCI DSS, as a result customers have to use this document only as a reference as it cannot serve as any basis for PCI DSS certification.

The introduction of HUAWEI CLOUD's products and services is only based on the current offering to the day when this document was published. Functions described in this document may change along products' updates, and specific product current descriptions on HUAWEI CLOUD's official website shall prevail.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.4 Basic definition

PCI Security Standards Council: The open global forum created by American Express, Discover Financial Services, JCB international, MasterCard International and Visa in 2006.

Cardholder Data (CHD): Cardholder data includes:

- Primary Account Number (PAN): generally a bank card number. Most credit card account numbers are 16 digits long;
- Cardholder Name: the owner's name registered on the primary account or any person authorized to use the card;
- Expiration Date: the authorization period of the bank card;
- Service Code: a 3 to 4 digits code used to identify service attributes, international and domestic data exchanges, usage restrictions, and so on.

Sensitive Authentication Data (SAD): Sensitive authentication data includes:

- Full Track Data: the data stored in the magnetic stripe at the back of credit cards. Each magnetic stripe has three tracks, respectively storing the PAN, name, expiration date, service code, CVV, PVV and other data;
- Credit Card Security Code: bank card security verification code, generally 3 to 4 digits long. Common security codes include CVV2 (VISA), CVC2 (Master Card), CVN2 (China UnionPay), CID (American Express), CAV2 (Japan JCB), etc.;
- PIN/PIN Block: Typically credit card transaction passwords.

Cardholder Data Environment (CDE): The person, process, or technology that stores, processes, or transmits Cardholder Data or Sensitive Authentication Data.

Customer: Refers to a registered user in a business relationship with HUAWEI CLOUD.

Service Provider: PCI defines a service provider as a commercial entity other than a payer that is directly involved in the processing, storage, and transmission of cardholder data, or an entity that provides services that affect the security of cardholder data.

Cloud Service Provider: A cloud service provider is a subclass of a service provider. Since only the use of HUAWEI CLOUD services is described within this practical guide, the use of the formulation cloud service provider, namely HUAWEI CLOUD, refers to the service provider formulation in the official documentation.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Introduction to PCI DSS

2.1 Standard Introduction

The PCI Security Standards Association is committed to the continuous development, improvement, storage, popularization and implementation of account data security standards. A total of three standards were released: Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PED Requirements.

The PCI DSS includes six areas: build and maintain a secure network and systems, protecting account data, maintaining vulnerability management plans, implementing strong access control measures, regularly monitor and test networks, and maintain an information security policy. The PCI DSS includes 12 specific security standard requirements. Provide a benchmark for the technology and operations used to protect account data and sensitive verification data.

Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls.
	2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data.
	4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software.
	6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know.
	8. Identify Users and Authenticate Access to System Components.
	9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data.
	11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

PCI DSS has become one of the leading certifications for global enterprises to demonstrate their data security capabilities, with the latest version of the standard version 4.0 released in 2022.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2.2 Standard Applicable

PCI DSS is applicable to all entities involved in payment card processing, including merchants, processors, acquirers, card issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit account data or sensitive verification data.

For customers whose business does not involve account data, you can also enhance their data protection capabilities by referring to the requirements of PCI DSS to comprehensively protect data security.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 PCI DSS Compliance by HUAWEI CLOUD

3.1 HUAWEI CLOUD Certification

Currently, HUAWEI CLOUD, as a cloud product and service provider, has obtained the PCI DSS certification based on version 4.0, indicating that the basic environment of HUAWEI CLOUD has met the requirements of PCI DSS and can provide customers with high-quality data security protection.

In addition, HUAWEI CLOUD will inevitably collect, transmit, and store customers' cardholder data during product or service provisioning. Therefore, HUAWEI CLOUD Operations Center, the department that processes customer cardholder data, has also passed the PCI DSS certification based on version 4.0, indicating that HUAWEI CLOUD can effectively protect customer cardholder data.

HUAWEI CLOUD has a global presence and operates 75 AZs in 29 regions (self-operated and jointly-operated), covering Asia Pacific, Latin America, Africa, Europe, and the Middle East. HUAWEI CLOUD provides products and services for customers around the world. Support customers to collect, transmit, and store cardholder data information according to their requirements.

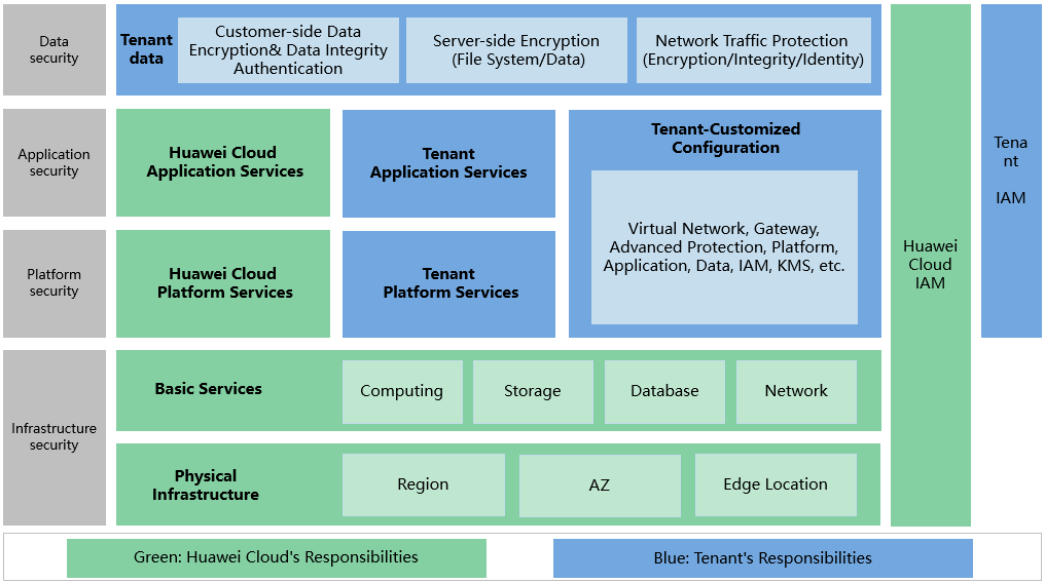
The compliance certification scope of the PCI DSS covers all cloud services provided by HUAWEI CLOUD on the HUAWEI CLOUD official website. For details, see the official website.

3.2 Huawei Cloud Security Responsibility Sharing

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:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-1 Responsibility Sharing Model



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

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

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

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

3.3 How HUAWEI CLOUD Meets PCI DSS Requirements

HUAWEI CLOUD strictly follows the requirements stated in PCI DSS, and sets corresponding data protection measures from the systems to processes in order to protect the cloud environment and the security of account data when customers purchase products and services on HUAWEI CLOUD's official website.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Secure networks and systems

This domain covers **requirements 1 and 2** listed in the standard, including installing and maintaining network security controls and applying secure configurations to all system components to establish secure systems and networks.

According to PCI DSS first requirement on network segmentation, HUAWEI CLOUD formulates the process and mechanism for installing and maintaining network security control and applications at the management layer. At the technical layer, HUAWEI CLOUD is not only using a firewall to isolate CDE from the system environment of other internal functions, but also uses load balancing, DNS and Web application firewall to filter external traffic and intercept it if unauthorized. Moreover, HUAWEI CLOUD has built its own secure virtual network (SVN) using its self-developed VPN, only allowing data sent using IPsec and VPN methods to further ensure the effectiveness and security of network isolation. HUAWEI CLOUD also has a Web upload whitelist to prevent unauthorized data to be uploaded.

HUAWEI CLOUD clearly requires databases or other system components not to use vendor-supplied default password, and if there are multiple default accounts, unnecessary accounts should be disabled or deleted accordingly.

Protect Cardholder Data

Protection of cardholder data is covered in the **requirements 3 and 4** mainly through the implementation of storage protection and encryption mechanisms.

HUAWEI CLOUD services and products are not collecting any cardholder data while being used. However, when customers purchase HUAWEI CLOUD products and services, they need to use the services of an online payment system or add their payment card information to process the payment. At this occasion, HUAWEI CLOUD will collect, transmit and store customers' cardholder data. As HUAWEI CLOUD attaches great importance to the security of cardholder data, AES encryption is used to store the cardholder account (PAN), partly covering PAN when needed to be displayed to the point where only the first 6 digits and last 4 digits are visible. To achieve the storage minimization, the cardholder data will be deleted once it's no longer needed or reach the retention period. Finally, sensitive authorized data would deleted immediately and consequently not stored after the payment has been verified.

In accordance with the standard, HUAWEI CLOUD uses cryptographic to encrypt, transmit and store customers' cardholder data in order to protect its security when being transmitted or stored. In addition, HUAWEI CLOUD uses the industry-standard TLS high version on the Transport Layer and IPsec protocols when transmitted the data. HUAWEI CLOUD also ensures secure transmission channels or AES encryption are used when transmitting sensitive data through untrusted networks. HUAWEI CLOUD has implemented a key management system to encrypt and manage cryptographic keys. The strength of the data encryption key (DEK) and key encryption key (KEK) are all defined by the AES encryption algorithm, which the PCI Security Standards Council considers as a strong encryption algorithm.

Vulnerability Management Plan

This domains corresponds to **requirements 5 and 6** of the standard, which ensure data security protection through the deployment of antivirus software, vulnerability management, and secure development and updates of systems and applications.

HUAWEI CLOUD uses intrusion prevention systems (IPS), Web application firewall, anti-virus software and host intrusion detection system (HIDS) to manage system components and network vulnerabilities. IPS can detect and prevent potential network intrusion events; Web application firewalls are deployed at the network boundaries to protect the security of an application software, so that it is not vulnerable to external SQL injection, CSS, CSRF and other application-oriented attacks; Antivirus software are installed to provide virus protection and a firewall for windows internal system; HIDS protects the security of cloud servers, reducing the risk of account theft, detecting weak passwords and malicious program, providing two-factor authentication, vulnerability management, webpage tamper-proof and other capabilities. Additionally, HUAWEI CLOUD regularly scans its environment to reduce the risk of having undiscovered security vulnerabilities.

To reduce risks related to vulnerabilities, HUAWEI CLOUD has established a security vulnerability management process, appointed a vulnerability manager and other related security roles responsible for vulnerability assessment, and ensure the regular installation of critical security patches.

Information security is included at every stage of HUAWEI CLOUD's products and services development life cycle. Before the release of a new version, the code of products is required to be reviewed and approved by a code auditor based on its security.

Implement strong access control measures

According to **requirements 7, 8 and 9**, the standard establishes access control measures from three aspects: user access identification, access permission control, and physical access permission control.

In the course of operations, HUAWEI CLOUD sets up the access rights to personal data based on employees' roles, uses an identity authentication system to restrict unauthorized access, and manages employees' permissions following the least-privilege approach, in order to avoid the illegal modification and disclosure of any personal data by employees.

HUAWEI CLOUD also provides strict protection controls for its employees' accounts such as enforcing account password's minimum length and complexity requirements, timely disabling inactive accounts, limiting the number of incorrect credentials submissions by locking accounts after a previously set-up number of failed attempts requiring the account owner to log in use multi-factor authentication to unlock his account.

In terms of physical protection of its equipment, HUAWEI CLOUD has selected locations for its data centers based on the principle of caution and has established special internal regulations to control the security within the building and infrastructures perimeters. Security management system, intrusion alarm system and video monitoring system are deployed in data centers. HUAWEI CLOUD does not only limit to the minimum the privileges of on-site operation and maintenance personnel, suppliers and internal staffs, but also strictly monitors

external visitors and personnel's access. Data breach prevention management is carried out not only when a physical storage media enters or leaves the computing room, but also when data should be erased or scrapped to prevent data loss or unauthorized disclosure incidents.

Monitoring and network test

This domain covers **requirements 10 and 11**. HUAWEI CLOUD monitors the system and regularly tests its related effectiveness in order to meet those requirements.

HUAWEI CLOUD uses both CLS log system to monitor system components by collecting, storing and analyzing records, and the independently CIP centralized security incident management system to analyze security incidents and provide real-time alarm capacities. The system performs intelligent analysis based on rules defined by threat models and experts. HUAWEI CLOUD also regularly reviews logs and treating measures of security incidents.

By monitoring critical infrastructures and networks, HUAWEI CLOUD has the capacity to timely detect possible network attacks and avoid data breach incidents. HUAWEI CLOUD has established a response process to network security incidents including the involvement of multiple departments cooperating to timely monitor the incidents and quickly deploy disposal measures to reduce its impact.

Information Security Policy

The establishment and maintenance of a comprehensive information security policy is listed in **requirement 12**.

HUAWEI CLOUD has established a series of data security policies and processes guidelines, and consequently obtained a variety of data security certifications, such as ISO 27001 information security management system, ISO 27017 cloud service information security management system, ISO 20000 information technology service management system certification, ISO 22301 business continuity management system, CSA STAR cloud security international gold certification, the International Common Criteria (CC) EAL3+ security assessment standard. HUAWEI CLOUD has also obtained a range of regional security certifications such as the MTCS Level3 Multi-Tier Cloud Security (Singapore), Certification for the Capability of Protecting Cloud Service User Data (China), Classified Cybersecurity Protection (China), Gold Operation and Management Certification Assessment of Trusted Cloud (China), Cloud Service Security Certification by Cyberspace Administration of China (China).

For each products and services' business units, the information security responsibilities of all employees corresponding to their roles are clearly defined. HUAWEI CLOUD has defined privacy and security protection roles having several responsibilities related to information security management. Moreover, HUAWEI CLOUD strictly processes background checks for its new employees and regularly conducts training and tests on security awareness, network security and privacy protection to enhance employees' understanding of data security in order to develop their data protection abilities and regulate their daily behaviors.

Regarding service providers' data security management, HUAWEI CLOUD has signed the "Supplier Network Security and Data Processing Agreement" with relevant service providers, which requires suppliers to comply with laws and

regulations related to personal data protection, and to establish a security protection system and security emergency response mechanism.

4 HUAWEI CLOUD Helps Customers Respond to PCI DSS Requirements

4.1 PCI DSS Assessment Guide

Customers can deploy a cloud environment compliant with PCI DSS on HUAWEI CLOUD. However, this does not mean that customers meet the compliance requirements of PCI DSS by default while using HUAWEI CLOUD. Customers and HUAWEI CLOUD share responsibilities related to data security based on the previously described responsibility matrix, and customers should take corresponding measures according to their business situation. If a customer wishes to be certified by PCI DSS, they will need to contact a Qualified Security Assessor authorized by the PCI Security Standards Council, called QSA, which will evaluate all system components contained in or connected to the cardholder data environment.

4.2 Standard requirements and specific measures

When a customer uses HUAWEI CLOUD to deploy its own cloud environment to process account data, the customer and HUAWEI CLOUD need to share the data security protection responsibility. This section describes how HUAWEI CLOUD, as a service provider, helps customers meet PCI DSS requirements.

Requirement 1 Install and Maintain Network Security Controls

PCI DSS recommends using a firewall to control computer access traffic between the internal network and the external network (untrusted network) and incoming and outgoing traffic in sensitive areas of the internal network, and to inspect all network traffic to prevent transmissions that do not meet established security standards. This prevents system components from being accessed by unauthorized users from untrusted networks.

Firewalls are deployed on HUAWEI CLOUD to filter the traffic between the external network and the internal network of HUAWEI CLOUD. Firewalls are responsible for infrastructure network settings and separate customer traffic from

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

management traffic. In this way, network isolation and tenant separation are implemented.

Requirement 1	
Customer Type	**Practical Guidelines for Customers**
IaaS	Customers are responsible for securing networks within and between their own environments through deploying firewalls to control the in and out traffic, and ensuring only trusted components are connected by identifying all networks, equipment and systems within the account data environment and other environments.
PaaS	Customers shall deploy firewalls in their platform environment to ensure the network security, and regularly check the list and settings of services, protocols, and interfaces that can access their environment.
SaaS	HUAWEI CLOUD is primary responsible for the network security protection.

To meet requirement 1, HUAWEI CLOUD provides customers with products such as **Virtual Private Cloud (VPC)**, **Cloud Firewall (CFW)**, and **NAT gateway**.

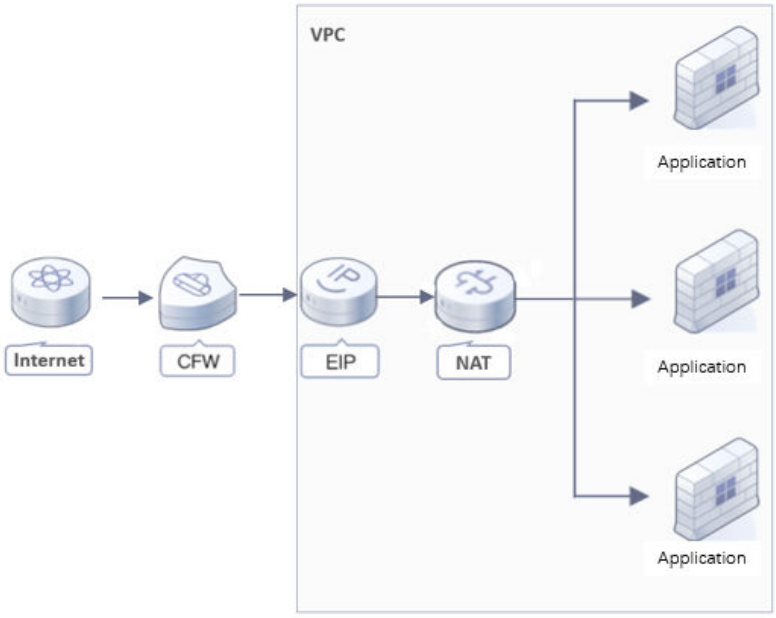
IaaS and PaaS customers can use VPC products to establish isolated and private virtual network environments on the cloud. Users can access the network smoothly and isolate tenants. In addition, VPC interconnection and interworking can be flexibly configured. VPCs are applicable to three scenarios, including dedicated networks on the cloud, web services, and hybrid clouds. VPCs are deployed to isolate the account data environment from other service environments and management environments. Implement the account data environment components in the account data environment cannot be directly public access through the Internet, and respond to the regulation in ***requirement 1.3*** that direct access between the Internet and the account data environment is prohibited.

CFW provides protection for the Internet border and VPC border on the cloud. As shown in the following figure, the CFW is located between the external Internet and VPC on the cloud. It provides the following functions: global unified access control, visualized full-traffic analysis, and real-time intrusion detection and prevention. Log audit and source tracing analysis, and on-demand elastic capacity expansion. Response ***requirement 1.3*** Restricting network access to the cardholder's data environment and ***requirement 1.4*** Controlling network connections between trusted and untrusted networks.

NAT gateway products are classified into public network NAT gateways and private network NAT gateways. The public network NAT gateway can translate private IP addresses into public IP addresses. After the translation, cloud resources can securely access the public network or provide services externally, and private network information is not directly exposed to the public network. The private network NAT gateway provides the private network address translation function to enable communication between VPCs and between VPCs and local data centers

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

(IDCs). It can meet to the ***requirements 1.4.5*** for hiding internal IP address and routing information.



Requirement 2 Apply Secure Configurations to All System Components

The default passwords or default settings provided by the vendor may be used illegally to threaten the security of the cloud environment, system, and software. Therefore, customers need to change default passwords, remove unnecessary software, functions, and accounts, and disable or remove unnecessary services.

HUAWEI CLOUD is responsible for the password configuration policies for infrastructure (only IaaS users) and system (IaaS and PaaS users) management accounts in the cloud environment, controls the password complexity and change period based on HUAWEI CLOUD password policies, and formulates applicable system configuration standards for system components.

Requirement 2	
Customer Type	**Customer practice guide**
IaaS	Customers are responsible for the security configuration of their systems, applications, and virtual system components deployed on HUAWEI CLOUD.
PaaS	
SaaS	HUAWEI CLOUD is responsible for the security configuration of devices, systems, and applications.

To meet **requirement 2**, HUAWEI CLOUD provides customers with products such as **Identity and Access Management (IAM)** and **Host Security Server (HSS)**.

When using IAM to create a user, the customer administrator can send an email to the new user. The new user needs to set a password when using the link to log in.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

In addition, the customer administrator can force the user to change the default password after activation. Both methods prevent IAM users from using the default password, and meet to the ***requirement 2.2*** for managing the default account of the vendor. In addition, the access to the IAM console using the customer account is transmitted over the public network using HTTPS. According to the meet ***requirement 2.2***, strong encryption is used to encrypt all non-console management accesses.

HSS is a dedicated security manager for servers. It provides functions such as asset management, vulnerability management, baseline check, and intrusion detection, helping enterprises manage host security risks and detect and prevent hacker intrusions in real time. HSS asset management includes the management and analysis of security asset information such as accounts, ports, processes, web directories, and software. It can meet the ***requirement 2.2*** for check whether only necessary services, protocols, daemons, and functions are enabled and all unnecessary functions are deleted or disabled.

Requirement 3 Protect Stored Account Data

The customer shall store account data to the minimum extent and use methods such as encryption and masking to protect account data to reduce the risk of unauthorized access and disclosure of account data.

For IaaS and PaaS customers, HUAWEI CLOUD mainly ensures the security of the infrastructure or platform provided by the customers to protect the stored account data.

Requirement 3	
Customer type	**Customer practice guide**
IaaS	The customer manages the encryption mechanism, storage method, and storage period of the data, and conceals the PAN.
PaaS	
SaaS	Determine the value based on the specific HUAWEI CLOUD products or services used by the customer.

To meet ***Requirement 3***, HUAWEI CLOUD provides customers with products such as **Cloud Databases**, **Data Encryption Workshop (DEW)**, and **Data Security Center (DSC)**.

HUAWEI CLOUD provides customers with a variety of cloud databases, including MySQL, PostgreSQL, SQL Server, distributed multi-mode NoSQL database, and has passed 14 domestic and international security compliance certifications such as ISO 27001, CSA, Trusted Cloud, etc. Cloud databases support connection with VPC to ensure the isolation of databases storing CHD from other operational environment. Customers can manage the retention period of cardholder data in a cloud database and securely erase data as needed and thus meeting ***requirement 3.1*** regulations on data retention, storage duration, and data deletion. SHA256 hashing capacity is provided for password authentication on the client side and server side of cloud database products. Moreover, logs are prohibited to display passwords or sensitive data through the implementation of security controls, which meets ***requirement 3.4*** the PAN is masked during displays.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Cloud databases support DEW hosting server-side encryption keys, helping customers to easily create and control their encryption keys by using hardware security modules (HSM) to secure key hosting. Customers' keys do not appear in plaintext outside of the HSM to avoid any kind of breach incident. Access control and log monitoring are carried out for all operations involving keys, such as providing usage records of every key, thus meeting ***requirement 3*** the provisions of PAN not readable.

The DSC provides basic data security capabilities, such as data classification, data security risk identification, data watermark source tracing, and static data anonymization. The DSC integrates the status of each phase of the data security lifecycle through the data security overview and displays the overall data security posture on the cloud. The DSC uses the in-depth behavior identification engine to establish user behavior baselines, implement real-time alarms for abnormal operations beyond the baseline, identify risk events, and optimize the source tracing audit chain. In addition, the DSC detects security violations in data use in a timely manner and generates alarms in a timely manner to prevent data leakage. Customers can also use more than 20 preset masking rules or user-defined rules to statically anonymize data. In addition, the data watermark injection/extraction function is used to trace data sources. It can meet the ***requirement 3*** for protecting the stored account data.

Requirement 4 Protect Account data with Strong Cryptography During Transmission Over Open, Public Networks.

Account data and sensitive information must be encrypted when transmitted over public networks. In addition, correct wireless networks and new encryption and verification protocols must be configured to protect data from easy access.

For IaaS customers, Huawei is responsible for the security protection during encrypted account data transmission. For PaaS users, HUAWEI CLOUD is responsible for the security protection of underlying transmission outside the customer's environment based on the service level agreement signed with customers.

Requirement 4	
Customer type	**Customer practice guide**
IaaS	The customer is responsible for specifying the transmission mechanism for account data and selecting the encryption and transmission technologies to be used. The customer also needs to ensure data security by encrypting data transmitted between public network components. And make sure that the wireless network that transmits account data or connects to the cardholder's data environment uses strong encryption.
PaaS	The customer is responsible for specifying the transmission mechanism for account data and selecting the encryption and transmission technologies to be used. The customer also needs to encrypt data transmitted between public network components to ensure data security.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Requirement 4	
SaaS	Determine the value based on the specific HUAWEI CLOUD products or services used by the customer.

To meet ***requirement 4,*** HUAWEI CLOUD provides customers with products such as **Elastic Load Balance (ELB)**, **Data Encryption Workshop (DEW)**, and **Direct Connect (DC)**.

ELB is a traffic distribution control service that distributes access traffic to multiple backend ECSs based on forwarding policies. It expands the external service capabilities of application systems and improves the fault tolerance capability of applications. ELB applies to encrypted transmission scenarios. This section describes how to configure security policies based on HTTPS listeners, including the TLS protocol version and matching encryption algorithm suites. Customers can configure TLS1.2 and TLS1.3 to enhance data transmission security and meet the ***requirement 4.2*** to use strong encryption methods to protect data security.

Requirement 4.2 also specifies the management of keys and certificates. Customers can use the HSM component in DEW to manage keys and set key strength to meet the requirements of the standard.

Customers can use DC to build high-speed, low-latency, stable, and secure dedicated connection channels between their local data centers and VPCs on HUAWEI CLOUD to ensure data transmission security between the data centers and VPCs. It can meet the ***requirement 4.2*** that end-user communication technologies, such as e-mail and instant messaging, are not used to transmit unprotected bank accounts.

Requirement 5 Protect All Systems and Networks from Malicious Software.

Malware, such as viruses, worms, Trojan horses, spyware, ransomware, etc., can enter corporate networks through employee email (e.g., via phishing) and through the use of the Internet, mobile computers, and storage devices, taking advantage of system vulnerabilities to cause loss. All systems should therefore use an anti-malware solution to protect against current and evolving malware threats.

HUAWEI CLOUD deploys an anti-malware solution for its server or platform and correctly configures its settings to maintain the effectiveness of anti-malware.

Requirement 5	
Customer type	**Customer practice guide**
IaaS	The customer is responsible for securing their operating system and its virtual machines and needs to deploy an anti-malware solution in their operating system to protect the account data environment from malware attacks.
PaaS	Customers need to deploy an anti-malware solution in their operating systems to protect their systems from malware attacks.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Requirement 5	
SaaS	HUAWEI CLOUD is responsible for anti-malware protection for the account data environment.

HSS uses advanced AI and machine learning technologies and integrates multiple antivirus engines to deeply detect and kill malicious programs on hosts, identify malicious programs such as backdoors, Trojan horses, and worms, and automatically isolate and kill malicious programs. In addition, HSS supports the detection of known ransomware viruses. This feature helps users automatically identify and process security risks in the system. It can meet the ***requirement 5.2*** to prevent or detect and dispose of malware.

Requirement 6 Develop and Maintain Secure Systems and Software

A security vulnerability may allow others to illegally obtain system access privileges, and all system components must have all appropriate software patches to prevent exploitation and threats to account data by malicious individuals and malware. For custom software, many vulnerabilities can be avoided through the Application Software Lifecycle (SLC) process and secure coding techniques.

HUAWEI CLOUD is responsible for protecting the security of device maintenance and patching in the customer's cloud environment or platform, and the development security of underlying applications. In PaaS and SaaS modes, HUAWEI CLOUD is responsible for the patch security and management of systems and applications based on the service type.

Requirement 6	
Customer type	**Customer practice guide**
IaaS	The customer shall ensure that the patches and updates of the operating system and applications are installed in a timely manner, take responsibility for the secure development of the operating system and applications, and maintain the appropriate change process.
PaaS	
SaaS	The customer should ensure that the patch or update has been installed in a timely manner.

To ***meet requirement 6***, HUAWEI CLOUD provides customers with products such as **Database Security Service (DBSS)**, and **Web Application Firewall (WAF)**.

Customers can also choose DBSS. Based on the machine learning mechanism and big data analysis technology, DBSS provides database audit, SQL injection attack detection, and risky operation identification functions, and also responds to SQL injection prevention and vulnerability identification requirements in ***requirement 6.1***.

The PCI DSS standard requires the installation of automated technical solutions that check and prevent web-based attacks in front of public-facing web

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

applications, continuously inspecting all traffic. Customers can purchase WAF to detect and defend website service traffic from multiple dimensions. As shown in the preceding figure, WAF can prevent attacks such as SQL injection and cross-site scripting, and provides four functions: data leakage prevention, vulnerability fixing, CC attack prevention, and web page tampering prevention. Deploy automated technical solutions in response to public-facing web applications in standard ***requirement 6.4*** to continuously detect and prevent attacks on web applications.

Requirement 7 Restrict Access to System Components and Account data by Business Need to Know

Best practice requires limiting personnel access to account data based on knowledge and job responsibilities, and appropriate systems and processes are used to ensure that access is properly set to prevent unnecessary or non-authorized personnel from accessing core and sensitive data.

All types of customers need to work with HUAWEI CLOUD to manage access control. HUAWEI CLOUD is responsible for access control of underlying infrastructure.

Requirement 7	
Customer Type	**Customer practice guide**
IaaS	It is the Customer's responsibility to define the rights of its different employees to access Account data and control over data access.
PaaS	
SaaS	It is the Customer's responsibility to define access to Account data by its different employees.

To meet ***requirement 7***, HUAWEI CLOUD provides IAM and other services for customers.

After a customer registers a HUAWEI CLOUD account, the IAM is enabled by default to provide identity authentication and permission management functions for the customer. After federated identity authentication is configured, IAM can directly access HUAWEI CLOUD from the enterprise management system, simplifying management. In addition, the system supports the permission management mechanism based on the customer group. The operation permission of a resource can be granted to an individual based on the project. The system can meet the ***requirements 7.2*** for assigning permissions based on the job classification and functions and the minimum permissions required for performing job responsibilities.

Requirement 8 Identify Users and Authenticate Access to System Components

Assign a unique identifier (such as an ID) to each person who has access, ensuring that each person is responsible for their actions. Once this accountability is in place, known authorized customers and processes perform operations and tracking on critical data and systems.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

The PCI DSS requires the establishment and management of strong authentication for users and administrators, such as the use of strong passwords/passwords. The validity of passwords depends largely on the design and implementation of the authentication system, especially the frequency with which attackers are allowed to try passwords and the security methods used to protect customer passwords at the point of entry, during transmission, and in storage. The standards also require the implementation of multifactor authentication (MFA) to ensure secure access to CDE and prevent abuse.

HUAWEI CLOUD uses a strong and effective verification mechanism in the management and control of underlying infrastructure. In addition to the IaaS mode, HUAWEI CLOUD retains the access control management permission on HUAWEI CLOUD system servers.

Requirement 8	
Customer type	**Customer practice guide**
IaaS	The customer shall control the of all accounts to ensure that each account has a unique ID and a strong and effective verification mechanism.
PaaS	
SaaS	The customer should assign unique IDs to their employees and adjust and disable their privileges based on their activity status.

As required by requirement 7, HUAWEI CLOUD provides IAM and other services to manage access control of customer personnel.

IAM also allows you to set the account lockout policy, account suspension policy, and session timeout policy that meet customer requirements. After the account lockout policy is set, the account will be locked if the number of failed login attempts reaches the preset value within a specified period. The number of failed login attempts can be set to 3 to 10. It can meet ***requirement 8.3.4*** indicates that the account will be locked if the number of failed login attempts does not exceed 10. If the number of failed login attempts reaches the maximum within the specified period, the account will be locked for a period of time. The lockout period can be set to 15 to 30 minutes. In the response, the lockout period described in ***requirement 8.3.4*** must be set to at least 30 minutes. IAM supports an inactive period ranging from 1 to 240 days. If an account does not log in within the specified period, the account will be disabled. The response is to the requirement of disabling an inactive account for 90 days specified in ***requirement 8.2.6***. If no operation is performed during the session within the specified duration, the user needs to log in again. The session timeout duration of IAM can be set from 15 minutes to 24 hours. The response requirement is as specified in ***requirement 8.2.8.*** If the session is idle for more than 15 minutes, the user needs to log in again. In addition, IAM allows users to change the password upon the first login. The password validity period and password complexity can be set to a value ranging from 1 to 180 days. In addition, the new password must be different from historical passwords. For details about the password complexity and password update rules, see ***requirement 8.3.4 to 8.3.9***.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

HUAWEI CLOUD IAM also supports multi-factor authentication and virtual MFA authentication for accounts, which can respond to the requirements in ***requirements 8.4 and 8.5*** related to the authentication mechanism.

Requirement 9 Restrict Physical Access to Account data

Where there is actual access to cardholder data or to the system in which it is stored, there is an actual risk of a data breach incident occurrence. Therefore PCI DSS requires that the auditee, here the customer, shall place appropriate physical restrictions to protect the data, the system, and the media in which cardholder data is stored.

However, due to the nature of cloud services, for all types of customers, there is no physical access control for cardholder data located in the cloud environment. As a cloud service provider, HUAWEI CLOUD is responsible for protecting its physical environment by controlling the physical access of its internal staff and external personnel to HUAWEI CLOUD's data centers, and ensuring data security protection during storage, transfer and disposal of any storage media. For the detailed protection measures taken by HUAWEI CLOUD, please refer to the section "Implement Strong Access Control Measures" in Chapter 3.2 of this document.

Requirement 10 Log and Monitor All Access to System Components and Account data

Logging mechanisms and the ability to track user activities are critical to preventing, detecting, or mitigating the impact of data threats. Logs exist in all system components and the Account data Environment (CDE) for comprehensive tracking, alerting, and analysis when errors occur.

HUAWEI CLOUD is responsible for infrastructure monitoring and log recording. SaaS customers need to rely on HUAWEI CLOUD monitoring and logs to manage and trace access activities.

Requirement 10	
Customer Type	**Customer practice guide**
IaaS	The customer is responsible for activity monitoring and system component logging for their own cloud environment.
PaaS	
SaaS	The customer is responsible for setting and monitoring logs at the application layer.

To meet requirement 10, HUAWEI CLOUD provides customers with services such as **Log Tank Service (LTS), Database Security Service (DBSS), Cloud Eye (CES), Managed Threat Detection (MTD), and Situational Awareness (SA)**.

LTS provides the functions of collecting, querying, and storing logs in real time. It records activities in the cloud environment for easy query and tracing. CES monitors login logs in real time. When a malicious login occurs, an alarm is generated and requests from the IP address are rejected. Based on the machine

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

learning mechanism and big data analysis technology, DBSS provides database audit, SQL injection attack detection, and risky operation identification functions. In addition, LTS and DBSS can record and store logs of system components for customers to review logs to meet the requirements specified in ***requirement 10.2*** "Check Logs" to detect abnormal and suspicious activities and collect evidence for events.

Logs recorded in the LTS can be dumped to OBS. After being dumped, logs can be stored for a long time. The retention period of logs is at least 12 months in ***requirement 10.5.1.***

MTD continuously checks whether visitors' IP addresses or domain names in the logs contain potential malicious activities and unauthorized behaviors by accessing IAM logs, DNS logs, CTS logs, OBS logs, and VPC logs generated by users performing operations on HUAWEI CLOUD in the target region. An alarm will be reported in time if any exception is found. This service integrates the AI intelligence engine, threat intelligence, and rule baseline capabilities to detect multiple cloud services. (including IAM, DNS, CTS, OBS, and VPC services) Abnormal access behavior hidden in log data proactively detects potential threats and generates alarms for potential threat access behaviors. Users can check and handle alarm information based on alarm description, handle potential threats in a timely manner, and upgrade and harden service security before major losses such as information leakage are caused, protecting user account security and ensuring stable service running. It can meet he ***requirement 10.4*** for using automated mechanisms to perform inspection log audits can be responded.

SA provides a unified threat detection and risk handling platform, helping users detect typical security risks encountered by cloud assets, restore attack history, detect attack status, predict attack posture, and provide powerful security management capabilities before, during, and after events. SA can collect statistics on the security status of core assets such as ECSs and VPCs on the cloud. The score deduction items are divided into four dimensions: security service enablement, threat alarm, baseline anomaly, and vulnerability. The known threat events, vulnerabilities, and possible threats encountered by assets are considered. All-round risk evaluation is performed around the clock, and the number of threat alarms, vulnerabilities, and baseline check exceptions and risk severity (critical, high, and medium) distribution are displayed in a centralized manner. Details can be drilled down to quickly handle the risks. It can meet ***requirement 10.2*** Implement log checks to support monitoring of abnormal and suspicious activities and forensic analysis of events.

Requirement 11 Test Security of Systems and Networks Regularly

System components, processes, and custom software should be tested frequently to ensure that security controls are appropriate for the changing environment.

Vulnerability scanning and penetration testing for underlying facilities and SaaS services are regularly organized and operated by HUAWEI CLOUD. Customers only need to test their cloud environment systems and processes.

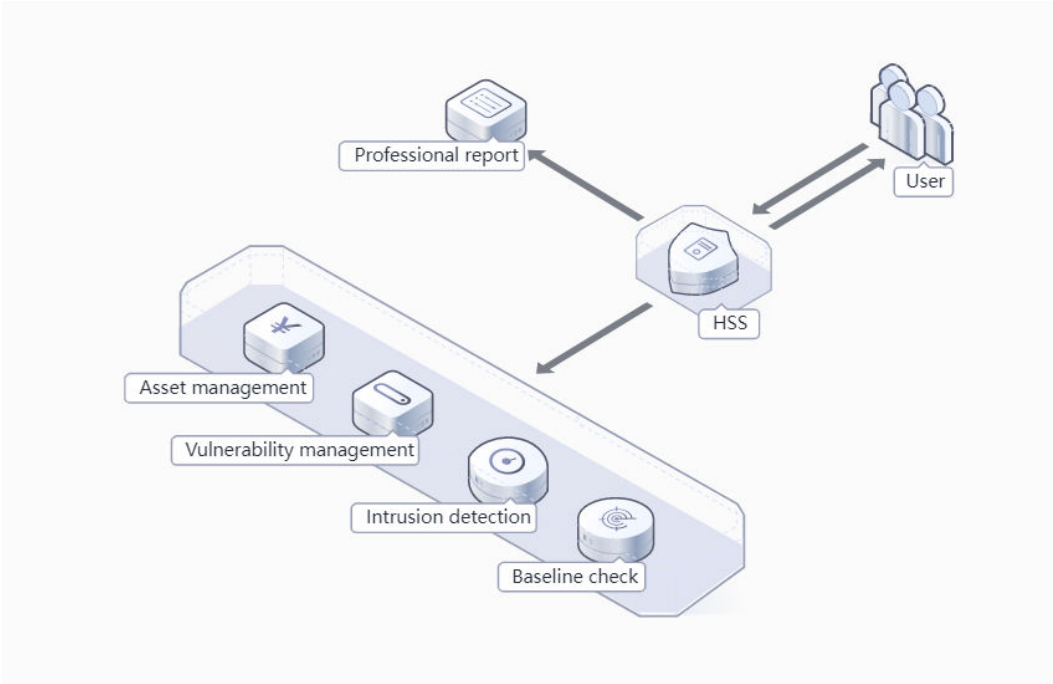
Requirement 11	
Customer Type	**Customer practice guide**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Requirement 11	
IaaS	The customer should negotiate with HUAWEI CLOUD about the support for functions such as intrusion detection and penetration testing. However, the customer needs to retest the security periodically or after a major change in the system or control.
PaaS	
SaaS	HUAWEI CLOUD is responsible for the security tests of systems and processes.

To meet ***requirement 11***, HUAWEI CLOUD provides customers with services such as **Host Security Service (HSS) and Web Application Firewall (WAF)**.

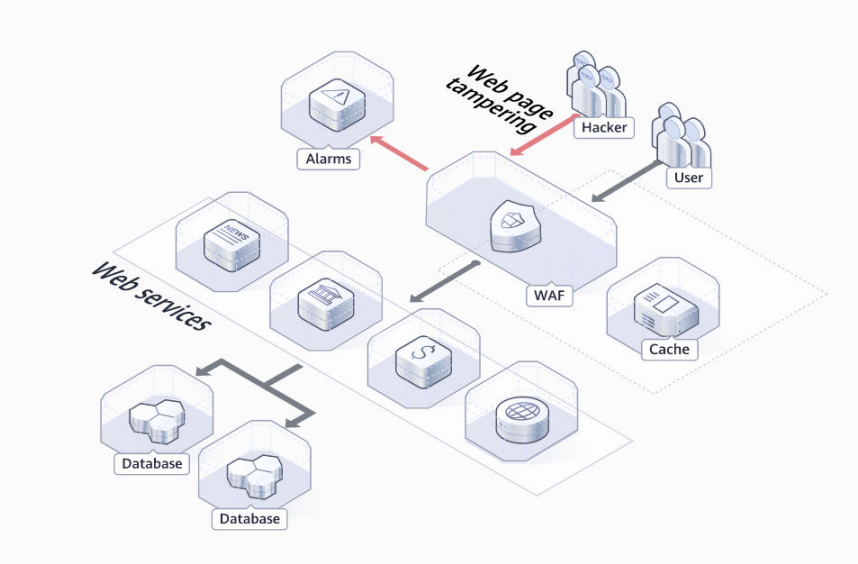
Customers can use HSS to evaluate host system security, display accounts, ports, software vulnerabilities, and weak password risks in the existing system, and prompt customers to perform security hardening to eliminate security risks and improve overall host security. The HSS also provides the intrusion detection function. When detecting an event, such as brute force cracking, abnormal process, or abnormal login, the HSS quickly generates an alarm. With the event management function, customers can obtain comprehensive information about alarms and events, helping customers detect security threats in assets in a timely manner and understand the security status of assets. It can respond to the requirements of ***requirement 11.5*** for the use of intrusion detection techniques to detect and prevent intrusions into the network.



In addition, the WAF can be used to prevent web pages from being tampered with. WAF supports Trojan horse detection to detect malicious code injected by malicious attackers on website servers, protect website visitors, prevent pages from being tampered with, protect page content security, and prevent attackers from tampering with pages, modifying page information, or releasing malicious

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

information on web pages. The website brand image is affected. With the web page anti-tamper function of the HSS, the payment page deployment change and tampering detection mechanism ***requirements 11.6.1*** are met.



Requirement 12 Support Information Security with Organizational Policies and Programs

Sound and effective security policies can protect information security more comprehensively. Employees' understanding of the company's security policies will effectively reduce risks caused by insufficient security awareness and irregular operations. All employees should be aware of the sensitivity of account data and their responsibility to protect such data.

HUAWEI CLOUD is responsible for formulating its own information security policies and providing regular training for employees to enhance their awareness and capabilities about data protection. During the actual operation, HUAWEI CLOUD needs to adjust the scope of responsibilities based on the service level agreement signed with the customer.

Requirement 12	
Customer Type	**Customer practice guide**
IaaS	The customer shall establish and maintain its own security policies and internal process system, define roles and responsibilities for security control, and provide training on data security for employees.
PaaS	
SaaS	

Customers should develop appropriate security policies and process guidelines based on their business and scale. HUAWEI CLOUD does not provide customers with relevant services or documents. Customers can establish their own information and data security systems by referring to ISO 27001 information security system and ISO 27018 cloud privacy protection certification standards.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3 List of applicable products

The following table summarizes the HUAWEI CLOUD products and services mentioned above and the main PCI DSS standard requirements to which the HUAWEI CLOUD products and services can respond.

Product name	Function Description	Corresponding standard requirements
Virtual Private Cloud (VPC)	Builds an isolated virtual network environment for resources such as ECSs, cloud containers, and cloud databases. Customers can configure and manage the virtual network environment.	1.4, 6.5
Cloud Firewall (CFW)	Provides cloud-based Internet and VPC border protection, including real-time intrusion detection and prevention, global unified access control, full-traffic analysis visualization, log audit, and source tracing analysis.	1.2, 1.3, 1.4, 10.3
NAT Gateway	Provides the NAT service for ECSs in a VPC or servers in the local data center connected to the VPC through Direct Connect or VPN.	1.4
Host Security Service (HSS)	The can comprehensively identify and manage information assets on hosts, monitor risks on hosts in real time, and prevent unauthorized intrusions.	2.2, 5.2, 5.3, 6.1, 11.5, 11.6, 10.3
Cloud Database (MySQL, PostgreSQL, SQL Server, GeminiDB)	The cloud database features out-of-the-box, stability, reliability, secure running, elastic scaling, easy management, and cost-effectiveness.	1.4.4, 3.2, 3.4

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Product name	Function Description	Corresponding standard requirements
Elastic Load Balance (ELB)	A traffic distribution control service that distributes access traffic to multiple backend servers and expands external service capabilities of application systems through traffic distribution.	2.2.7, 4.2
Data Encryption Workshop (DEW)	Provides dedicated encryption, key management, and key pair management services.	3.3, 3.5, 3.6, 3.7, 4.2
Direct Connect (DC)	This feature enables customers to establish a dedicated connection channel between their on-premises data centers and VPCs on the cloud to implement secure and reliable hybrid cloud deployment.	1.4、4.2
Database Security Service (DBSS)	Provides the database security audit service in off-line mode and generates alarms in real time for risky and attack behaviors.	6.1, 10.2
Web Application Firewall (WAF)	By detecting HTTP/HTTPS requests, it identifies and blocks malicious attacks and ensures the security and stability of web services.	6.4, 10.3, 10.7, 11.6
Identity and Access Management (IAM)	Provides identity authentication and permission management functions, manages customer accounts, and controls the resource operation rights of these customers.	7.2, 7.3, 8.2, 8.3, 8.4, 8.5
Log Log Service (LTS)	Provides log collection, real-time query, and storage functions. Users can use logs for real-time decision-making analysis without development.	10.2, 10.5, 10.7
Cloud Eye (CES)	Provides a multi-dimensional monitoring platform for resources such as ECSs and bandwidth.	10.7

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Product name	Function Description	Corresponding standard requirements
Managed Threat Detection (MTD)	MTD continuously detect malicious activity and unauthorized behavior to protect accounts and workloads.	10.2、10.4、10.7、10.5、11.5、11.6
Cloud Bastion Host (CBH)	Provides host management, permission control, O&M audit, and security compliance functions, and supports remote O&M anytime and anywhere on mainstream browsers such as Chrome.	3.4.2、7.3、8.4、8.5、8.6
Data Security Center Service (DSC)	Provides basic data security capabilities, such as data classification and grading, sensitive data scanning, data security check, data watermark source tracing, and data anonymization.	3.2.1, 3.4.1, 3.5
Situation Awareness (SA)	This feature helps users detect typical security risks of cloud assets, restore attack history, detect attack status, and predict attack posture, providing powerful security management capabilities before, during, and after events.	2.2、10.2、10.4、10.5、10.7、11.5、11.6
Cloud Certificate Manager (CCM)	CCM is a service for issuing and managing cloud certificates throughout the lifecycle. Currently, it provides SSL certificate management and private certificate management services.	4.2

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Conclusion

HUAWEI CLOUD always adheres to HUAWEI's "customer-centric" core values and commit to protect customers data security resulting in the establishment of an information security management system and the deployment of the most common data security protection technologies in the industry to ensure customers data security.

Simultaneously, in order to help customers cope with the increasingly openness and complexity of network environments and the development of new information security technologies, HUAWEI CLOUD continuously develops various products, services and solutions in the field of data protection to support customers in improving their data protection ability and reducing their risks.

This white paper is for reference only and does not have any legal effect or constitutes legal advice, nor does it serve as a basis for certain compliance of customers' account data environment when using HUAWEI CLOUD. Customers should evaluate their own operation and certification requirements, selecting appropriate cloud products and services, and properly configuring them.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 References

No.	Posted by	Document Name
1	PCI Security Standards Association	Payment Card Industry (PCI) Data Security Standard Requirements and Testing Procedures Version 4.0
2	PCI Security Standards Association	PCI Security Standards Association Cloud Computing Guidelines (April 2018)

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7 Version History

Date	Version	Description
February 2023	**3.0**	**Eligibility Requirements Update**
April 2022	2.0	Eligibility Requirements Update
July 2020	1.0	Initial release

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.