Alibaba Cloud PCI DSS
Responsiblity Management Matrix

September, 2020

Table of Contents

1 Executive Summary

Alibaba Cloud (Singapore) Private Limited or Alibaba Cloud Computing Ltd., also known as "Alibaba Cloud" is an independent Cloud Computing Service Provider (CSP) provides the capability for clients utilizing Alibaba Cloud' processing capacity, storage, networks, and other fundamental computing resources. The type of services including Infrastructure as a Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Alibaba Cloud services do not directly store, process, or transmit cardholder data and sensitive authentication data, and the PCI compliant environment facilitates customers' PCI DSS compliance (i.e. the products or systems do not enforce implementation or configuration settings that violates a PCI DSS requirement).

atsec (Beijing) Information Technology Co., Ltd (Hereinafter referred to as "atsec") the Qualified Security Assessor (QSA) company validated that Alibaba Cloud has completed Payment Card Industry Data Security Standard (PCI DSS) V3.2.1 assessment for Public Cloud International Services and Public Cloud Services. The detail information about the Attestation of Compliance is described as below:

- Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020.
- Attestation of Compliance for Alibaba Cloud Security Services Products issued by atsec on August 5, 2020.
- Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020.
- Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on November 2, 2020.

Intended Use: This document is intended to be used by Alibaba Cloud customers to understand the scope of the Alibaba Cloud PCI DSS assessment and expectations for responsibilities when using Alibaba Cloud services as part of the customer's cardholder data environment.

For customers to meet PCI DSS compliance while using Albiaba Cloud services, please refer "Section 4 PCI DSS Requirements and Responsibility Management Matrix For Alibaba Cloud Customer" below.

2 Alibaba Cloud PCI DSS Compliance Description

Alibaba Cloud Management Environment is the underlying physical and logical infrastructure that supports the Alibab Cloud services including servers, operating systems, hypervisor and control environment for management and operations of the Alibaba Cloud service.

The Alibaba Cloud Management Environment and the following services were included in the PCI DSS compliance assessment.

2.1 Alibaba Cloud Management Environment

2.1.1 Physical Security

All of the Alibaba Cloud data center and office areas are configured with access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by Alibaba Cloud staff when visiting Alibaba Cloud premises. Alibaba Cloud data centers are all in compliance with the requirements for Class A in the GB 50174 Code for Design of Electronic Information System Room and the T3+ standards in the TIA-942 Telecommunications Infrastructure Standard for Data Centers, including the following requirements for physical and environmental security control:

2.1.1.1 Data center disaster recovery

- **Fire detection and response**
- **Power**
- **Temperature and humidity**

2.1.1.2 Personnel Management

- **Access management**

  At each Alibaba Cloud data center, long-term access permissions are assigned only to corresponding maintenance personnel. If an employee is transferred to another position or leaves the company, access permissions of the employee are cleared immediately. If it is necessary for any other person to enter the data center, the person must submit a formal application in advance, and is granted temporary permission only upon the approval of the corresponding department heads. For each entry to or exit from the data center, such persons must display their ID to check in, and be escorted by the data center's maintenance personnel for the entire duration of the visit.

  An Alibaba Cloud data center consists of equipment rooms, electrical measurement areas, warehouses, and other areas, with each area equipped with an independent access control system. Two-factor authentication (such as biometric verification) is employed for sensitive areas, and special areas are physically isolated by metal cages.

  All Alibaba Cloud data centers and office areas have access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by Alibaba Cloud staff when visiting Alibaba Cloud premises.

- **Account management and identity authentication**

Alibaba Cloud uses a central account management and identity authentication system to manage employee accounts throughout their lifecycle.

- **Authorization management**

  Alibaba Cloud grants minimum resource access permissions to employees based on their positions and roles while ensuring separation of duties. An employee can log on to the central permission management platform to apply for access permissions to VPN Gateway, Bastion Host, control platforms, and production systems as needed. The requested permissions are granted to the employee upon the approvals of the supervisor, data or system owner, security administrator, and relevant departments.

- **Separation of duties**

  Alibaba Cloud separates duties between O&M permissions by role to prevent permission violations and audit failures. Duties are separated between O&M and audit staff, with the security team being responsible for the audit. Duties are also separated between the database and system administrators.

2.1.1.3 O&M audit

- **Surveillance**

  Alibaba Cloud data centers and server rooms are equipped with security surveillance systems covering all the areas and passages, and staffed with security guards for 24/7 patrol. All the surveillance videos and documents are saved and reviewed by dedicated personnel on a regular basis.

- **Audit**

  All the maintenance operations on the production system can only be performed with Bastion Host. The entire operation process is recorded in logs, which are then transferred to a central logging platform in real time. Alibaba Cloud defines audit rules for violations in accordance with its Account Usage Specifications and Data Security Specifications. Any violations will be handled by security personnel accordingly.

  Internally, all the sensitive operations are logged in the management system that has a browser/server (B/S) structure, as stated in Alibaba Cloud log audit specifications, and such logs are transferred to the central logging platform. The central logging platform provides only the APIs for collecting and reading, not for modifying and deleting logs.

2.1.1.4 Data destruction

- **Secure erasure**

  Alibaba Cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, and reuse or decommissioning. Access control and operation monitoring of devices are managed strictly, and maintenance and stocktaking of devices are conducted on a regular basis. When any device is recycled or decommissioned, Alibaba Cloud takes data erasure measures for the storage media. Prior to disposal of data assets, it is necessary to check whether the media containing sensitive data and genuine licensed software has been overwritten, degaussed, or physically bended and destroyed to make sure that the data cannot be restored. When certain hard copy materials are no longer needed due to business or legal reasons, Alibaba Cloud physically destroys them or obtains proof of destruction from any third-party data processors, to ensure that the data cannot be reconstructed.

- **Disposal of cloud service customer data**

  On terminating services to cloud service customers, Alibaba Cloud deletes the data assets of the customers in a timely manner or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are logged to prevent unauthorized access to customer data.

2.1.1.5 Network isolation

Alibaba Cloud isolates production networks from non-production networks. Direct access from a non-production network to any servers and network devices in a production network is not allowed. Alibaba Cloud isolates the cloud service network that provides services to external users from the physical networks that supports the underlying cloud service functionalities. Network ACLs are configured to prohibit access from cloud service network to physical network. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from initiating external connections.

Alibaba Cloud deploys Bastion Host on production network boundaries. The O&M personnel in the office network can access the production network for O&M only through Bastion Host. When logging on to Bastion Host, O&M personnel must perform multi-factor authentication, namely a one-time password is required apart from the regular domain account name and password. Bastion Host uses advanced encryption algorithms to ensure the confidentiality and integrity of data transmitted through O&M channels.

2.1.2 Hardware security

2.1.2.1 Firmware security

Secure firmware is one of the foundations for overall cloud computing security. The firmware used within the Alibaba Cloud infrastructure is securely hardened. Such hardening techniques include firmware baseline scanning, high-performance GPU instance protection, BIOS secure update, and BMC firmware protection.

- Firmware baseline scanning: The version and other related information of hardware and firmware are scanned on a regular basis for any potential exceptions.
- High-performance GPU instance protection: This technique provides protection to critical GPU registers so that the GPU flash cannot be modified by the users’ virtual machines, and sensitive assets such as the GPU's firmware cannot be tampered with.
- BIOS secure update: This technique ensures that only the BIOS images signed by Alibaba Cloud are flashed to the servers to avoid BIOS-level attacks such as malicious BIOS flashing.
- BMC firmware protection: This technique prevents unauthorized BMC firmware flashing in the host operating system.

2.1.2.2 Encrypted computing

Alibaba Cloud platform uses Intel® Software Guard Extensions (Intel® SGX) to provide a hardware-trusted execution environment. Users can establish a trusted execution environment to protect their sensitive data such as encryption/decryption keys. The root of trust in cryptographic computing is based on the processor chip, not on the underlying software. Therefore, all encrypted information can only be computed and run in a trusted execution environment, providing a high level of hardware-based data protection.

2.1.2.3 Trusted computing

Alibaba Cloud uses trusted computing technology to provide trust at the system and application level. Specifically, security critical servers use TPM 2.0-based security measurement and verification to ensure a secure computing environment. Furthermore, to ensure the security of trusted applications, Alibaba Cloud monitors and manages a trusted application whitelist on security critical applications.

TPM 2.0 and vTPM technologies are used to measure the underlying software stack on physical machines and VMs during the boot up process, and the trusted computing technology is used to verify the measurement results. The underlying software being measured includes BIOS, BootLoader, OS kernel, and loaded system modules and applications. Security O&M personnel can determine whether the system can be trusted by verifying the measurement results and taking the corresponding security responses such as reinstalling the correct software version or performing business migration.

The trusted computing technology can also record and analyze the execution behaviors of an application, such as process startup, file access, and network access, and creates its behavior whitelist and model. When the application is running, the service dynamically measures the collected application behaviors and compares the measurement results with the permissible actions in the whitelist to determine whether the application can be trusted. Based on the verification results, the security O&M personnel can take measures such as reinstalling the correct application version.

2.1.3 Virtualization security

Virtualization technology is the foundation of cloud computing. It ensures isolation between multiple tenants in a cloud computing environment by means of virtualized computing, storage, and network. Alibaba Cloud virtualization security technology mainly involves five security features, namely tenant isolation, security hardening, escape detection, hotfix patching, and data erasure.

2.1.3.1 Tenant isolation

Virtualization plays a crucial role in tenant isolation. Based on the hardware virtualization technology, VMM allows VMs on multiple computing nodes to be isolated from each other at the system layer. It prevents unauthorized access to system resources between tenants and guarantees basic computing isolation between computing nodes. The virtualization management layer also provides storage isolation and network isolation.

- **Computing isolation**

  Alibaba Cloud provides a variety of cloud-based computing instances and services that allow automatic scaling to meet application or business needs. These computing instances and services provide computing isolation at multiple levels to protect data while ensuring configuration flexibility. The key isolation boundaries are between the management system and VMs, and between VMs themselves. Such isolation is provided by the hypervisor. Alibaba Cloud platform uses a virtualized environment where ECS instances run as standalone VMs and the isolation is enforced by using different permission levels (i.e. ring levels) of physical processors to avoid unauthorized access of a user's VM to the host and to another VM.

- **Storage isolation**

  In the basic design of cloud computing virtualization, Alibaba Cloud separates VM-based computing from storage. This separation allows computing and storage to be scaled independently, and makes it easier to provide multi-tenant services. At the virtualization layer, the

hypervisor substitutes a virtual device for its physical equivalent storage device. All the I/O operations of a VM are intercepted by the hypervisor to ensure that the VM can only access the physical disk space allocated to it, thus implementing security isolation of hard disk space between different VMs.

- **Network isolation**

  To provide network connections for ECS instances, Alibaba Cloud connects the instances to the Alibaba Cloud virtual network. Alibaba Cloud's virtual network is a logical structure built on top of the physical network structure. All the logical virtual networks are isolated from each other. Such isolation prevents network traffic data from being snooped or intercepted by other malicious instances.

2.1.3.2 Security hardening

Security hardening refers to the use of various technical means to reduce the possible attack surface in the hypervisor. Alibaba Cloud uses a lightweight KVM-based hypervisor developed specifically for cloud computing. The hypervisor combines the needed hardware and software capabilities by design, and focuses on supporting only hardware virtualization for the cloud infrastructure underneath. To reduce the potential impact of zero-day vulnerabilities, the Alibaba Cloud hypervisor limits the number of calls to system-level dynamic libraries without affecting functionality or performance. In summary, Alibaba Cloud minimizes the amount of code that is not related to devices on the cloud at the hypervisor level, therefore reducing the attack surface. In addition, all virtualization software must be compiled and run in a trusted execution environment to ensure that each binary file is not maliciously altered or replaced during runtime. Alibaba Cloud uses a series of trusted computing technologies to ensure the security of the entire virtualization software stack, and provides a complete set of control mechanisms to ensure that these virtualization software binary files are not accessible by external malicious parties.

Alibaba Cloud also hardens security at the hypervisor and host OS/kernel levels. For example, hypervisor permissions are downgraded during dynamic runtime, and the kernel is prevented from executing user space code. This increases the difficulty of permission escalation after an escape. Memory address layout randomization, restricted kernel symbol access, and memory page protection features are implemented to increase the difficulty of memory overflow type attacks. Alibaba Cloud continues to introduce new security features into the hypervisor and host OS/kernel, including the latest security features developed by Alibaba Cloud and the open source community.

2.1.3.3 Escape detection

The Alibaba Cloud hypervisor uses advanced VM distribution algorithms to prevent malicious VMs from running on a targeted physical machine. VMs cannot proactively detect the physical host environment in which they are located. At the hypervisor level, Alibaba Cloud also detects abnormal VM behaviors (i.e. potential attack events) by performing the following operations: analyze and monitor Coredump files in real time, detect suspicious code snippets loaded and executed by the hypervisor in real time, audit VM calls to system functions and abnormal VM Exit behaviors, monitor and analyze possible abnormal behaviors such as irregular process execution and network behaviors of hosts.

When an attack is detected, Alibaba Cloud locates and discards the VM that initiated the attack, reconstructs the attack chain in a timely manner, and performs hotfix patching on any discovered vulnerabilities.

2.1.3.4 Hotfix patching

Alibaba Cloud virtualization platform supports hotfix patching technology, which can fix system defects or vulnerabilities without user intervention, thus keeping any negative effects on user business operations to a minimum.

2.1.3.5 Data erasure

Data erasure is an extension of storage virtualization. After an ECS instance is released, its original disk space and memory space are reliably scrubbed to ensure user data security.

2.1.4 Identity and access control

2.1.4.1 Identity management

Alibaba Cloud uses an identity authentication system to provide account lifecycle management for internal users such as regular employees, interns, outsourced employees, and partner employees. Each user is assigned a unique account, and the user must use such an account when dealing with corporate data. Once an account is assigned, the account cannot be shared, and unified logon management, password management, and access control of the account are enforced. When internal users leave Alibaba Cloud, move to new positions, or change their job responsibilities, the account resources used or managed by them must be revoked and/or transferred to proper Alibaba Cloud personnel.

2.1.4.2 Password management

Alibaba Cloud assigns each user a unique account, and each account has a clear owner. A unified password policy is employed. It requires users to configure a password that meets certain length and complexity requirements and to change the password on a regular basis (further, users are prevented from reusing their previous password). Multiple logon authentication modes are supported, such as account and password logon, one-time password logon, and digital certificate logon.

2.1.4.3 Permission management

Alibaba Cloud assigns permissions based on business needs, and centrally manages permissions by role, user group, department, and user. Each internal user can apply for and use permissions through the permission management system, and the permissions can also be revoked through the system. To strengthen permission management and reduce the risk of using incorrect permissions, Alibaba Cloud sets different levels of permissions and roles according to risks, and implements different approval processes accordingly at different permission levels. The system automatically freezes permissions that have not been used for a certain period of time. For users who leave Alibaba Cloud, the system automatically freezes their accounts and reclaims their permissions. For users who move to new positions, the system automatically revokes their permissions.

2.1.5 Security monitoring and operations

2.1.5.1 SPLC

Secure Product Lifecycle (SPLC) is a solution tailored for cloud products, designed to integrate security into the entire product development lifecycle. With SPLC, a complete security development mechanism is put into place at each stage, from product architecture review, development, validation, all the way up to incident response, to ensure that the products meet the rigorous security requirements for cloud computing. As a result, SPLC helps to greatly improve security capabilities and reduce security risks in cloud products.

2.1.5.2 Cloud platform security monitoring

The main purpose of security monitoring on the cloud platform is to promptly discover security incidents in which platform resources such as applications, hosts, and networks are attacked, and then trigger the internal incident response process to properly handle the incidents and eliminate potential impact.

Security monitoring mainly consists of three parts: log collection, anomaly analysis and detection, and alerting. Log collection aims to collect logs of hosts, networks, applications, and cloud products on the cloud platform, and import them into online real-time (such as Blink) and offline (such as MaxCompute) computing platforms. Anomaly analysis and detection aims to process and analyze the logs through security monitoring algorithms in each computing platform to monitor and identify risks. Once a security incident is discovered, an alert will be displayed on the security monitoring platform of Alibaba Cloud, and security emergency personnel will be notified via DingTalk (IM), SMS, or email to immediately handle the incident.

2.1.5.3 Penetration testing on the cloud platform

Alibaba Cloud has developed plans to conduct attack-and-defense drills on the cloud platform. During a drill, Alibaba Cloud organizes a specialized team of cyber penetration and attack experts to conduct security tests against Alibaba Cloud by means of periodic attack-defense confrontation. The drill is designed to objectively test the defense and threat detection capabilities of Alibaba Cloud, enhance the core security capabilities of Alibaba Cloud, and improve the security defense system.

2.1.5.4 Cloud platform incident response

Cloud platform incident response refers to actions taken by Alibaba Cloud in response to internally detected and externally reported vulnerabilities and security incidents. Internally, Alibaba Cloud discovers possible security incidents through log collection, anomaly analysis and detection, and alert generation. The external reporting channels include Alibaba Security Response Center (ASRC), Alibaba Cloud Crowdsourced Security Testing Platform, externally reported Common Vulnerabilities and Exposures (CVE) vulnerabilities of open source third-party components, and threat intelligence information from third parties.

Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered. The first step in incident response is to verify the authenticity of the reported vulnerabilities and security incidents. Once the vulnerabilities and security incidents are confirmed, Alibaba Cloud security team will initiate the incident response process and follow the standard protocols. The security severity level and impact scope of a vulnerability will be confirmed, and the response team will ensure resources are properly allocated so that the vulnerability can be fixed and the affected Alibaba Cloud product can be brought online within the corresponding SLA time. The steps to handle a security incident include confirming the impact scope of the incident, eliminating the impact, reviewing the incident, and making subsequent improvements. Meanwhile, the incident response team will promptly notify users of security issues through online announcements. Alibaba Cloud has a rigorous incident response process in place to ensure that every security incident is handled rigorously and quickly.

To ensure the effectiveness of the incident response process, Alibaba Cloud has set up a dedicated team to conduct attack drills from time to time. Alibaba Cloud also regularly invites third-party teams to conduct penetration testing on the Alibaba Cloud platform to verify the effectiveness of the Alibaba Cloud security protection system and the reliability of the incident response process.

2.1.5.5 Change management

The virtualization system is the foundation of cloud computing. Any changes to the virtualization system can directly affect cloud operations. Alibaba Cloud has established a comprehensive change management process based on ISO/IEC 20000, where changes are classified based on the degree of emergency and are managed by category based on their sources and targets. The criteria for judging possible outcomes from various changes are also clearly defined. The whole change process is standardized and is supported by automatic systems and tools. Any changes need to go through a series of phases from application, evaluation, approval, test, implementation, and finally to verification. The responsibilities of various personnel involved in the process are clearly defined.

- Application phase of change: Key actions, including application submission, documentation, reception, and approval, are clearly defined.
- Implementation phase of change: including the change scheme, plan, assessment, and implementation. All the changes are tested before being implemented. The change time window and change scheme are subject to strict review. In addition, Alibaba Cloud will send a change notice to customers who may be affected by such change. Important change operations must be reviewed and confirmed by two persons.
- Verification phase of change: including change verification, configuration item review, and change result notification. Alibaba Cloud records all the information throughout the change process and deploys an automatic configuration check tool to verify the configurations of infrastructure and information systems after a change.

2.1.6 Host Operating System

Alibaba Cloud manages and operates infrastructure (including but not limited to data centers deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), distributed cloud OS named Apsara, and various cloud services and products running on top of the Apsara OS. Alibaba Cloud protects the security of hardware, software, and network of the cloud platform by means of OS- and database-patch management, network access control, etc.

2.1.7 Authentication

Identity authentication refers to the use of account credentials to verify the real identity of a user. An account credential usually refers to a user's logon password or Access Key (AK). Alibaba Cloud provides the following authentication mechanism to complete the user's identity authentication:

- **Logon password**

  A user can use the logon password and user name of its Alibaba Cloud account or those of its RAM users to log on to the Alibaba Cloud console and perform operations on cloud resources.

- **Access Key**

  An Access Key (AK) is the credential used for calling Alibaba Cloud service APIs. It is used to authenticate the identity of users who access Alibaba Cloud resources through APIs.

- **STS**

  Alibaba Cloud Security Token Service (STS) is a cloud service that provides trusted entities such as RAM users, Alibaba Cloud services, and identity providers with authorization credentials for short-term resource access.

- **MFA**

  Multi-factor authentication (MFA) is a simple and effective security best practice that provides an extra level of protection on top of usernames and passwords.

- **SSO**

  Alibaba Cloud supports SAML 2.0-based Single Sign On (SSO), which enables enterprise users to access Alibaba Cloud (as the service provider) by using the logon service of the enterprise's identity system (as the identity provider).

2.1.8 Authorization

Alibaba Cloud provides a variety of tools and features to help customers securely authorize access to resources in different scenarios. Among them, the Resource Access Management (RAM) service is provided for user identity management and resource access control. RAM enables an Alibaba Cloud account (i.e. primary or root account) to have multiple independent RAM users (i.e. subaccounts). This eliminates the need for an account owner to share its Access Key or other credentials with other users, and the account owner can assign minimum operation permissions to different RAM users based on the principle of least privilege. RAM can be used to define fine-grained authorizations at an API operation or resource ID level. RAM also supports various restrictive conditions on permission granting, such as constraints on source IP address, required SSL/TLS channel, access time period, and MFA.

RAM is the basis for the security management and O&M of Alibaba Cloud accounts. RAM can assign a different password or API Access Key to each RAM user, which eliminates security risks arising from sharing of Alibaba Cloud account credentials. Assigning different work permissions to different RAM users also reduces the risks by following the principle of least privilege.

2.1.9 OpenAPI

Alibaba Cloud provides OpenAPI for cloud products / services to launch and terminate instances, perform other functions are all authenticated to an Alibaba Cloud account or role and signed for message integrity. In addition, OpenAPI calls can be encrypted with TLS to maintain security. Alibaba Cloud recommends always using TLS-protected API endpoints. Alibaba Cloud RAM also enables an Alibaba Cloud customer to further control what APIs a user has access to utilize.

2.1.10 Data Security

Customer data security and user privacy are the top most priorities of Alibaba Cloud. Alibaba cloud helps its customers to manage and control data security throughout the data lifecycle (production, storage, usage, transmission, propagation, and destruction).

2.1.10.1 Encryption at Rest and in Motion

Alibaba Cloud uses data encryption to ensure data security, including sensitive data encryption in applications, transparent data encryption in the RDS database, OSS encryption, hardware security modules, and encryption for network data transmission.

- **Data Encryption in Motion**

  The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud services provide customers with API access points with

HTTPS encryption enabled, allowing customers to use AccessKeys to call Alibaba Cloud Service API securely. Industry standard TLS protocol with 256-bit key length is used to address the need for encrypted transmission of sensitive data.

- **Data Encryption at Rest**

  Alibaba Cloud provides Key Management Service (KMS) for key management and data encryption capabilities for the encrypted storage of sensitive data on the cloud platform. Such sensitive data include authorization credentials, passwords, and encryption keys. In addition, data encryption is also enabled in different Alibaba Cloud products.

2.2 PCI DSS compliance In-Scope Services

Following are the service including in the PCI DSS assessment. Alibaba Cloud provides different cloud environments for different users. The different of Public Cloud International Services and Public Cloud Services is the IT infrastructure environments of Public Cloud Services are located in Mainland China and the infrastructure environments of Public Cloud International Services are located outside of Mainland China.

The detial descriptions of each service as described by Alibaba Cloud and derived from Alibaba Cloud website at https://www.alibabacloud.com/product/

Category	Name of Service	Public Cloud International Services	Public Cloud Services（Mainland China）
Cloud Essentials-Elastic Computing	**Virtual Server**		
	Elastic Compute Service (ECS)	Included	Included
	ECS Bare Metal Instance	Included	Included
	Elastic GPU Service	Included	Included
	Simple Application Server	Included	Included
	Dedicated Host	Included	Included
	High Performance Computing (HPC)		
	Elastic High Performance Computing (Elastic HPC)	Included	Included
	Super Computing Cluster (SSC)	Included	Included
	Container		

	Alibaba Cloud Container Service for Kubernetes	Included	Included
	Container Registry	Included	Included
	Elastic Orchestration		
	Auto Scaling	Included	Included
	Operation Orchestration Service (OOS)	Included	Included
Cloud Essentials-Network	**Cloud Network**		
	Virtual Private Cloud (VPC)	Included	Included
	Server Load Balancer (SLB)	Included	Included
	Elastic IP Address (EIPs)	Included	Included
	Network Address Translation (NAT) Gateway	Included	Included
	Cross Region Network		
	Cloud Enterprise Network (CEN)	Included	Included
	Hybrid Cloud Network		
	VPN Gateway	Included	Included
	Smart Access Gateway	Included	Included
	Express Connect	Included	Included
Cloud Essentials-Storage	**Cloud Storage**		
	Object Storage Service (OSS)	Included	Included
	Apsara File Storage NAS	Included	Included
	Tablestore	Included	Included

Cloud Essentials-Content Delivery	**Content Delivery**		
	Alibaba Cloud Content Delivery Network (CDN)	Included	Included
	Dynamic Route for Content Delivery Network (DCDN)	Included	Included
	Secure Content Delivery Network (SCDN)	Not Included	Included
Database	**Relational Database**		
	ApsaraDB for PolarDB	Included	Included
	Distributed Relational Database Service (DRDS)	Included	Included
	PolarDB-X	Not Included	Included
	ApsaraDB RDS for MySQL	Included	Included
	ApsaraDB RDS for PostgreSQL	Included	Included
	ApsaraDB for MariaDB TX	Included	Included
	ApsaraDB RDS for PPAS	Included	Included
	NoSQL Database		
	ApsaraDB for Redis	Included	Included
	ApsaraDB for MongoDB	Included	Included
	ApsaraDB for Memcache	Included	Included
	Data Warehouse		
	AnalyticDB for PostgreSQL	Included	Included
	Utility & Tools		

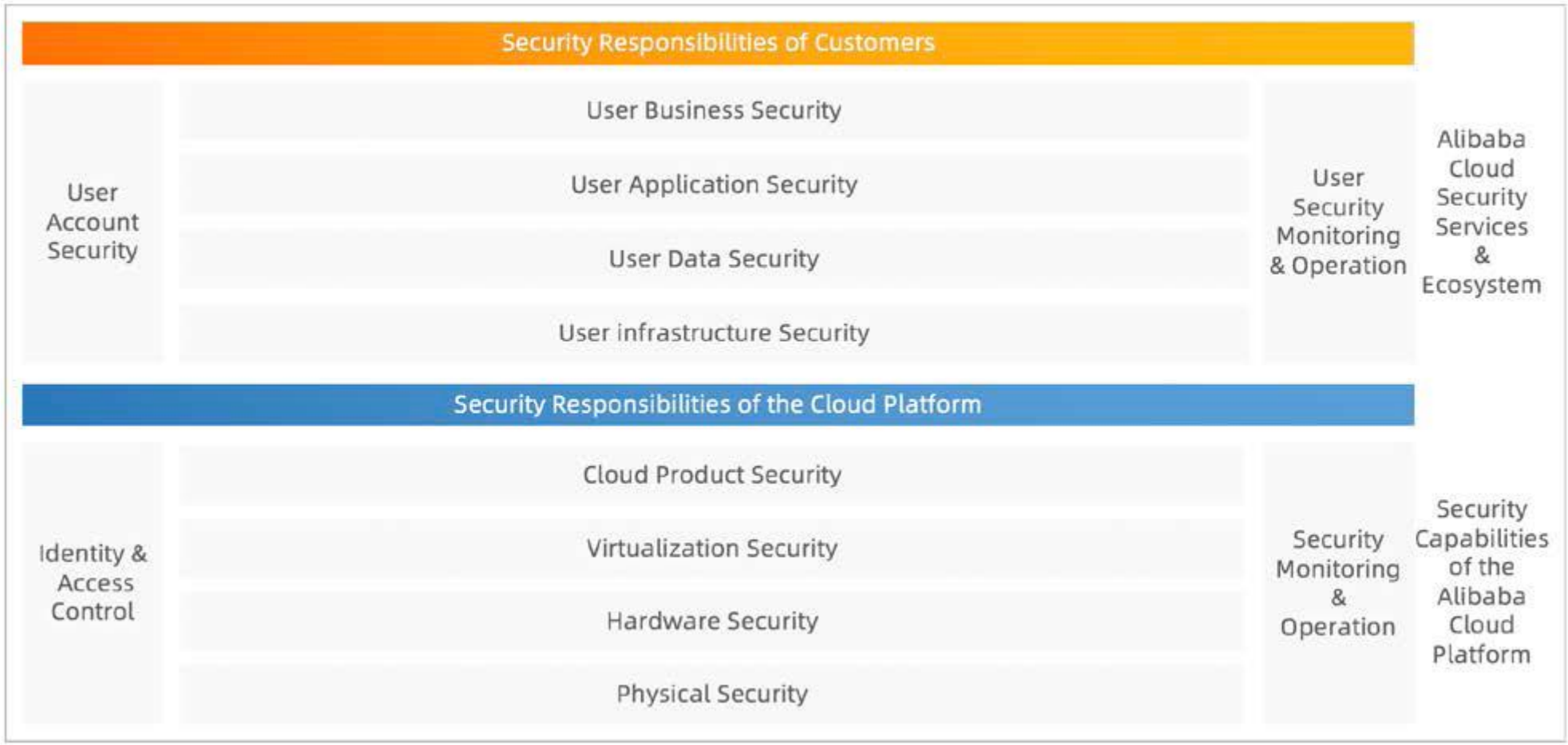
	Database Backup	Included	Included
	Data Management	Included	Included
Security	**Cloud Security**		
	Anti-DDoS Basic	Included	Included
	Anti-DDoS Pro	Included	Included
	Anti-DDoS Premium	Included	Included
	ActionTrail	Included	Included
	Cloud Config	Included	Included
	Cloud Firewall	Included	Included
	Web Application Firewall (WAF)	Included	Included
	BastionHost	Not Included	Included
	Security Center	Included	Included
	Cloud Security Scanner (CSS)	Not Included	Included
	Identity Management		
	Resource Access Management (RAM)	Included	Included
	Identity as a service (IDaaS)	Not Included	Included
	Data Security		
	Key Management Service (KMS)	Included	Included
	DBAudit	Not Included	Included
	Data Encryption Service	Not Included	Included
	Business Security		

	Content Moderation	Not Included	Included
Analytics	**Data Computing**		
	MaxCompute	Included	Included
	Data Search and Analytics		
	Elasticsearch	Included	Included
	Log Service	Included	Included
Artificial Intelligence	**Image**		
	Optical Character Recognition	Not Included	Included
Enterprise Applications	**Domains & Website**		
	Alibaba Cloud DNS	Included	Included
	Message Queue		
	AlibabaMQ for Apache Kafka	Included	Included
	Message Queue for Apache RocketMQ	Included	Included
	Micro Services		
	Enterprise Distributed Application Service	Included	Included
	Application Configuration Management	Included	Included
	Intelligent Services		
	Cloud Call Center	Not Included	Included
Developer Services	**Developer Services**		
	CloudMonitor	Included	Included

3 Alibaba Cloud Security Responsibilities Considerations

3.1 Alibaba Cloud Shared Security Responsibilities Model

The security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and its customers. Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services.



Alibaba Cloud must ensure the security of infrastructure (including but not limited to data centers deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), virtualization solutions, and cloud products running on top of the Apsara distributed cloud OS. Alibaba Cloud is also responsible for identity management and access control, monitoring, and operations of the platform to provide customers with a highly available and secure cloud service platform.

Customers must configure and use cloud products based on security best practices, and build applications on these securely configured cloud products. Alibaba Cloud offers Alibaba Cloud Security, which leverages the years of expertise in attack prevention technologies to help customers protect their applications and systems. Customers can choose to use Alibaba Cloud Security or any third-party security products in the Alibaba Cloud security ecosystem to protect their applications and business systems.

Alibaba Cloud employs a shared security responsibility model between itself and its customers, where Alibaba Cloud secures the cloud platform and provides integrated cloud security products and capabilities to customers. This relieves much of the underlying security burdens while allowing customers to focus more on their core business needs. Note that the Apsara Stack security responsibility model is somewhat different from the aforementioned public cloud security model. For more information, see Alibaba Cloud Apsara Stack Security White Paper.

3.1.1 Security Responsibilities of Alibaba Cloud

Alibaba Cloud is responsible for the security of its infrastructure, physical devices, Apsara OS, and cloud products/services, and provides customers necessary technical capabilities to protect their cloud applications and data. Alibaba Cloud secures its cloud platform from several aspects, including but not limited to:

- Protecting the physical security of cloud data centers;
- Protecting the security of hardware, software, and network of the cloud platform by means of OS and database patch management, network access control, Anti-DDoS, and disaster recovery, etc.;
- Identifying and fixing security vulnerabilities of the cloud platform in a timely manner without affecting customers' service availability;
- Cooperating with independent third-party security regulation and audit agencies to audit and evaluate security and compliance of Alibaba Cloud.

Alibaba Cloud provides customers with the technical means to protect cloud information systems, including but not limited to:

- Providing multihomed BGP access networks and cloud data centers distributed across multiple regions and zones, and allowing customers to build high availability cloud applications based on Alibaba Cloud infrastructure;
- Providing secure hardware infrastructure and equipment;
- Providing Alibaba Cloud account security management capabilities, including but not limited to the use of two-level account credentials (Alibaba Cloud accounts and RAM user accounts) for segregation of duties, multi-factor authentication (MFA), grouped authorization, fine-grained authorization control, and temporary authorization tokens;
- Providing security monitoring and operations capabilities, including security audits;
- Providing data encryption support;

- Providing various Alibaba Cloud security services;
- Working with third-party security vendors to provide customers with security solutions tailored to their needs.

3.1.2 Security Responsibilities of Customers

Customers who build cloud applications on Alibaba Cloud are responsible for protecting their own systems by using the security features provided by Alibaba Cloud products/services and the third-party security products in the Alibaba Cloud security ecosystem.

Customers' applications and business systems on Alibaba Cloud need to be protected by Alibaba Cloud Security services and any third-party security products in the Alibaba Cloud security ecosystem. Customers can also use Alibaba Cloud Security services to monitor and manage the security of applications and business systems on the cloud. Customers must protect their Alibaba Cloud account credentials by taking such measures as enabling MFA, granting only the minimum permissions required, and ensuring a separation of duties by means of assigning permissions by group. Furthermore, customers can use Alibaba Cloud ActionTrail to record OpenAPI calls and operations performed on the console, and audit account operations.

Customers must manage security configurations for cloud products/services to ensure infrastructure security and data security on the cloud. Customers have full control over infrastructure services such as ECS instances provided by Alibaba Cloud, and are responsible for managing these instances and performing the necessary security configurations. Customers must harden the OS on their ECS instances, install security patches in a timely manner, and properly configure security groups for network access control. For other Alibaba Cloud services, such as platform and cloud native services, customers do not need to maintain the underlying computing instances, such as keeping the OS updated, hardened, and patched. Instead, customers are only responsible for managing the service account authentication and resource authorization, and using the security features available with these services. For example, MaxCompute provides various levels of access control capabilities. Customers only need to configure security features in such products according to their business needs, configure source IP address whitelist for RDS, configure TLS protocol and encryption cipher suites for SLB/CDN, configure password policies for RAM, etc.

Customers can also use the native encryption capabilities of Alibaba Cloud products or Alibaba Cloud Data Encryption Service for security-sensitive data encryption, and use the managed Hardware Security Module (HSM) feature integrated with KMS for encryption key management.

Alibaba Cloud provides customers with a variety of security services and capabilities. In turn, customers are responsible for properly configuring and using these security services and capabilities to ensure the security of their applications and business systems on the cloud.

4 PCI DSS Requirements and Responsibility Management Matrix For Alibaba Cloud Customer

This section describes the Alibaba Cloud customers' responsibilities for leveraging the PCI validated Alibaba Cloud services in a compliant. The following defines the column headings for the PCI DSS Requirements and Responsiblity Management Matrix:

- **PCI DSS Requirements** – This column defines the Data Security Standard requirements; PCI DSS compliance is validated against these requirements.
- **Responsibility** – This column defines the PCI DSS responsibility for Alibaba Cloud and Customers. The responsibility categorize as "Alibaba Cloud", "Customer", and "Shared" respectively, indicate where the control originates. All controls originate from a system or from a business process. It is important to understand where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. Below are the definitions for each security control originates.
    - **Alibaba Cloud:** Alibaba Cloud is responsible in managing and maintaining the control to comply with PCI DSS requirement. Customers can use Alibaba Cloud Public Cloud International Service's Attestation of Compliance (AOC) to validate the scope.
    - **Customer:** Control that is solely the responsibility of the customer, based on the application being deployed within Alibaba Cloud services. Customer must validate compliance of such controls through their own PCI DSS program.
    - **Shared:** Control that is managed and implemented partially by Alibaba Cloud and partially by the customer. Both Alibaba Cloud and its customers own the responsibility to manage and maintain such controls to comply with PCI DSS.
- **Scope of Customer PCI DSS Responsibility** – This column describes the scope of customer PCI DSS compliance responsibility.
- **Scope of Alibaba Cloud PCI DSS Responsibility** – This column describes the scope of Alibaba Cloud PCI DSS compliance responsibility.
- **Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance** – This column describes how Alibaba Cloud will provide evidence of compliance to customers.

4.1 Build and Maintain a Secure Network and Systems

4.1.1 Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a

more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
1.1 Establish and implement firewall and router configuration standards that include the following:				
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**Shared**	**All In-Scope Services:** Customers are responsible for testing and approving their network connectivity and configuration for storing cardholder data in Alibaba Cloud services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX,**	**All In-Scope Services:** Alibaba Cloud is responsible for testing and approving the network connectivity and configuration for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher, OSS, VPC and Cloud Firewall: Customers are responsible for configuration of the network connections of their VM, database, or OSS instances (i.e., via Security Groups, VPC / Cloud Firewall ACLs, whitelist), and approval of the purchased Cloud services sharing port access with SLB, VPN Gateway, Smart Access Gateway, NAT Gateway CEN, CDN, SCDN, DCDN and Express Connect, etc.		
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining network diagrams for their Cardholder Data Environment (CDE).	N/A	N/A
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining the cardholder data flows for their Cardholder Data Environment (CDE).	N/A	N/A
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**Customer**	**All In-Scope Services:** Customers are responsible for creating DMZ, internal networks and other security zones by using VPC, Cloud Firewall or other firewall technologies.	N/A	N/A

		VPC and Cloud Firewall: VPC and Cloud Firewall are the compliance solution for customer to meet PCI DSS requirement 1.1.4. Customers are responsible for the VPC and / or Cloud Firewall policies deployment and configuration to creating DMZ and internal network.		
1.1.5 Description of groups, roles, and responsibilities for management of network components	**Shared**	**All In-Scope Services:** Customers are responsible for defining the roles and responsibilities for managing their Security Groups, whitelist, VPC / Cloud Firewall ACLs and any other network related configurations.	**All In-Scope Services:** Alibaba Cloud is responsible for defining the roles and responsibilities for managing the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**Shared**	**All In-Scope Services:** Customers are responsible for documenting the ports and protocols with justification for inbound and outbound access. Documentation should include network access configured in their security groups, whitelist, VPC / Cloud Firewall ACLs or other firewall technologies	**All In-Scope Services:** Alibaba Cloud is responsible for documenting the ports and protocols with justification for inbound and outbound access of the Alibaba Cloud Management Environment and Alibaba Cloud service	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on

		used for creating DMZ, internal networks and other security zones. Customers are responsible for identifying insecure services and implementing appropriate security controls and security features to mitigate the risk of the protocols from being used.	infrastructure. Alibaba Cloud are responsible for identifying insecure services and implementing appropriate security controls and security features to limit the risk of the protocols from being used.	September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.1.7 Requirement to review firewall and router rule sets at least every six months	**Shared**	**All In-Scope Services:** Customers are responsible for performing reviews of their access control that are used to filter traffic into the CDE every six months. This includes but may not be limited to: ■ ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, OSS, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcacher' Security Groups, VPC and / or Cloud Firewall ACLs and whitelist;	**All In-Scope Services:** Alibaba Cloud is responsible for performing reviews of their firewalls and other network technology and services that are used to filter traffic into the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure every six months.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		■ SLB, VPN Gateway, Smart Access Gateway, NAT Gateway CEN, CDN, SCDN, DCDN and Express Connect configuration		
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.				
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**Shared**	**All In-Scope Services:** Customers are responsible for implementing and configuring the Security Groups, VPC / Cloud Firewall ACLs, whitelist or other firewall technologies used to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. **VPC and Cloud Firewall:** VPC and Cloud Firewall are the compliance solution for customer to meet PCI DSS requirement 1.2.1. Customers are responsible for the VPC and / or Cloud Firewall policies deployment and	**All In-Scope Services:** Alibaba Cloud maintains instance isolation for Host Operating System and the Alibaba Cloud Management Environment including Host Operating System, Network Security, and Virtualization Security. Alibaba Cloud meets all PCI DSS requirements for implementing and managing access control for the Alibaba Cloud management environment and Alibaba Cloud service infrastructure. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server,**	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		configuration to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	**Dedicated Host, Elastic HPC and SCC, VPC and Cloud Firewall:** Alibaba Cloud Security Group, VPC and Cloud Firewall provide stateful inspection network access control and are suitable for compliant network segmentation.	
1.2.2 Secure and synchronize router configuration files.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers that use server-based technologies for implementing router and firewall rules are responsible for synchronizing and securing these technologies.	**All In-Scope Services:** Alibaba Cloud is responsible for synchronizing and securing the router configuration files used by Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**Shared**	**All In-Scope Services:** Customers that use wireless networks are responsible for isolating their cardholder data environment from those wireless networks.	**All In-Scope Services:** Alibaba Cloud maintains the perimeter firewalls and or ACLs to control traffic between wireless networks and systems in Alibaba Cloud data centers.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on

				September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.				
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**Shared**	**All In-Scope Services:** Customers are responsible for implementing and configuring the VPC / Cloud Firewall ACLs or other firewall technologies used to: ■ Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. ■ Restrict unauthorized outbound traffic from the cardholder data environment to the Internet. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible	**All In-Scope Services:** Alibaba Cloud maintains instance isolation for Host Operating System and the Alibaba Cloud Management Environment including Host Operating System, Network Security, and Virtualization Security. Alibaba Cloud meets all PCI DSS requirements for implementing and managing access control for the Alibaba Cloud management environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**Shared**			
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	**Shared**			
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**Shared**			

		for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks. **ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcached and OSS**: Customers are responsible for reviewing the connectivity models and exposure of their instances to these data stores, to ensure that appropriate zones are created, and to determine that access mechanisms to the data stores that have cardholder data are not directly exposed to the Internet. **VPC and Cloud Firewall:** VPC and Cloud Firewall are the compliance solution for customer to meet PCI DSS requirements 1.3.1, 1.3.2, 1.3.3 and 1.3.4. Customers are responsible for the VPC and / or Cloud Firewall policies deployment and configuration to restrict inbound and outbound traffic to that which is		

		necessary for the cardholder data environment .		
1.3.5 Permit only “established” connections into the network.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for ensuring the use of stateful inspection firewalls or mechanism to permit only “established” connection can access the public ports of ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, and SCC instances.	**All In-Scope Services:** Alibaba Cloud meets all PCI DSS requirements for implementing and managing access control for the Alibaba Cloud management environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**Customer**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for placing system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. **ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS**	N/A	N/A

		for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcached and OSS: Customers are responsible for reviewing the connectivity models and exposure of their instances to these data stores, to ensure that appropriate zones are created, and to determine that access mechanisms to the data stores that have cardholder data are not directly exposed to the Internet.		
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: ● Network Address Translation (NAT) ● Placing servers containing cardholder data behind proxy servers/firewalls, ● Removal or filtering of route advertisements for private networks that employ registered addressing, ● Internal use of RFC1918 address space instead of registered addresses.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for developing appropriate configuration on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances to prevent the disclosure of IP addresses and routing information. **NAT Gateway:** NAT Gateway is one of the compliance solution for customer to meet PCI DSS requirement 1.3.7. It's	**All In-Scope Services:** Alibaba Cloud is responsible for preventing the disclosure of IP Addresses and routing information for the Alibaba Cloud management environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		customers' responsible for deploying NAT Gateway service to prevent the disclosure of IP addresses and routing information for CDE		
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: ● Specific configuration settings are defined. ● Personal firewall (or equivalent functionality) is actively running. ● Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	**Customer**	**All In-Scope Services:** Customers are responsible for implementing firewall rules for systems with direct connectivity to the Internet for systems used to manage the CDE.	N/AAlibaba Cloud is responsible for preventing the disclosure of IP Addresses and routing information for the Alibaba Cloud management environment and Alibaba Cloud service	N/A
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	**Shared**	Customers are responsible for ensuring that their policies and procedures are documented and known to all affected	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020.

		parties.	documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.1.2 Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for changing vendor-supplied defaults on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC.	**All In-Scope Services:** Alibaba Cloud is responsible for the configuration and hardening standards deployment and maintenance for the Alibaba Cloud Management Environment that provides the virtualization technologies and applications for the cloud services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**Customer**	**All In-Scope Services:** Customers are responsible for management of their networks, including those with wireless connectivity.	N/A	N/A
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ● Center for Internet Security (CIS) ● International Organization for Standardization (ISO) ● SysAdmin Audit Network Security (SANS) Institute ● National Institute of Standards Technology (NIST).	**Shared**	**All In-Scope Services:** Customers are responsible for documenting the functional and security configuration standards of Alibaba Cloud services used within the CDE to ensure that the secure state designed for the service can be maintained. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcached:** Customers are responsible for documenting, developing and implementing configuration standards for the ECS, ECS Bare Metal	**All In-Scope Services:** Alibaba Cloud is responsible for the configuration and hardening standards deployment and maintenance for the Alibaba Cloud Management Environment that provides the virtualization technologies and applications for the cloud services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcached instances.		
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for ensuring that only one primary function is implemented per customer-managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instance.	**All In-Scope Services:** Alibaba Cloud is responsible for the configuration and hardening standards deployment and maintenance for the Alibaba Cloud Management Environment that provides the virtualization technologies and applications for the cloud services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	**Shared**	**All In-Scope Services:** Customers are responsible for documenting the functional and security configuration standards of Alibaba Cloud services used within the CDE to ensure that the secure state designed for the service can be maintained.	**All In-Scope Services:** Alibaba Cloud is responsible for the configuration and hardening standards deployment and maintenance for the Alibaba Cloud Management Environment that	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	**Shared**			
2.2.4 Configure system security	**Shared**			

parameters to prevent misuse.		**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcached:** Customers are responsible for documenting, developing and implementing configuration standards for the ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcached instances.	provides the virtualization technologies and applications for the cloud services.	Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**Shared**			
2.3 Encrypt all non-console administrative access using strong cryptography.	**Shared**	**All In-Scope Services:** Customers are responsible for encrypting all non-console administrative access with strong	**All In-Scope Services:** Alibaba Cloud is responsible for the configuration and hardening standards	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for

		cryptography for their self developed or implemented applications. Customers are responsible for using TLS 1.1 protocol or higher.in the cardholder data environment.. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for ensuring secure communication for administrative access to the ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC server instances including Windows Remote Desktop (RDP) using “High Encryption” or “FIPS compatible” encryption settings or SSH v2 or above and appropriate SSH keys. **SLB:** SLB is one of the compliance solution for customer to meet PCI DSS requirement 2.3. It’s customers‘ responsible for deploying SLB service with strong cryptography to protect non-console administrative access data flow.	deployment and maintenance for the Alibaba Cloud Management Environment that provides the virtualization technologies and applications for the cloud services (user web console and OpenAPI, etc.).	Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

2.4 Maintain an inventory of system components that are in scope for PCI DSS.	**Shared**	**All In-Scope Services:** Customers are responsible for maintaining an inventory of Alibaba Cloud resources that are in scope for their PCI DSS compliance.	**All In-Scope Services:** Alibaba Cloud is responsible for maintaining an inventory of Alibaba Cloud resources that are in scope for its PCI DSS compliance.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*	**Customer**	**All In-Scope Services:** Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. Customers are responsible for protecting their	N/A	N/A

		customer's data within Alibaba Cloud services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** The Secondary Shared-Hosting Provider is responsible for entities' hosted environments and ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC instances protection.		

4.2 Protect Cardholder Data

4.2.1 Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements ● Specific retention requirements for cardholder data ● Processes for secure deletion of data when no longer needed ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. **OSS:** OSS provides lifecycle policies for the stored content. Customers are responsible for the lifecycle policies configuration in accordance with this PCI DSS requirement when storing cardholder data in OSS.	N/A	N/A
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: ● There is a business justification and ● The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	N/A	N/A

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: ● The cardholder's name ● Primary account number (PAN) ● Expiration date ● Service code To minimize risk, store only these data elements as needed for business.	**Customer**			
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not- present transactions) after authorization.	**Customer**			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	**Customer**			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. Note: This requirement does not supersede stricter requirements in	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements.	N/A	N/A

place for displays of cardholder data—for example, legal or payment card brand requirements for point- of-sale (POS) receipts.				
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ● One-way hashes based on strong cryptography, (hash must be of the entire PAN) ● Truncation (hashing cannot be used to replace the truncated segment of PAN) ● Index tokens and pads (pads must be securely stored) ● Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI DSS requirements. **KMS and Data Encryption Service:** KMS and Data Encryption Service are the compliance solution for customer to meet PCI DSS requirement 3.4. Customers are responsible for deploying and configuring KMS and / or Data Encryption Service to protect their cardholder data information. Customers are also responsible for the creation, usage, and management of encryption keys in accordance with PCI DSS when using this service.	N/A	N/A

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. Note: This requirement applies in addition to all other PCI DSS encryption and key- management requirements.	**Share**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC provide disk encryption function for customer to meet PCI DSS requirement 3.4.1. Customers are responsible for enable the disk encryption function while creating the ECS instance if needed	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Alibaba Cloud is responsible for ECS disk encryption keys management and protection.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key- encrypting keys must be at least as strong as the data-encrypting key.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining encryption technologies, key management processes and cryptographic architecture for maintaining PCI DSS requirements.	N/A	N/A
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: ● *Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date*	**Customer**			

• *Description of the key usage for each key* • *Inventory of any HSMs and other SCDs used for key management*				
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**Customer**			
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times • Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method Note: It is not required that public keys be stored in one of these forms.	**Customer**			
3.5.4 Store cryptographic keys in the fewest possible locations.	**Customer**			
3.6 Fully document and implement all key- management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining encryption technologies and key management processes for maintaining PCI DSS requirements.	N/A	N/A

various resources including NIST, which can be found at http://csrc.nist.gov.		**KMS and Data Encryption Service:** KMS and Data Encryption Service are the compliance solution for customer to meet PCI DSS requirements 3.6.1 and 3.6.3. Customers are responsible for secure maintaining their cryptographic keys used for encryption of cardholder data according with industry standards.		
3.6.1 Generation of strong cryptographic keys	**Customer**			
3.6.2 Secure cryptographic key distribution	**Customer**			
3.6.3 Secure cryptographic key storage	**Customer**			
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**Customer**			
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification	**Customer**			

purposes.				
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	**Customer**			
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**Customer**			
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key- custodian responsibilities.	**Customer**			
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.2.2 Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: ● Only trusted keys and certificates are accepted. ● The protocol in use only supports secure versions or configurations. ● The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: ● The Internet ● Wireless technologies, including 802.11 and Bluetooth ● Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) ● General Packet Radio	**Shared**	**All In-Scope Services:** Customers are responsible for cryptography and security protocols configuration or implementation for connections to any storage system that is transmitting cardholder data. Customers are responsible for ensuring the data is encrypted in transit as well as when stored. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for configuring their self deployed web servers with security TLS protocols, using strong encryption ciphers and trusted certificates to safeguard	**All In-Scope Services:** Alibaba Cloud encrypts access and manages encryption within the Alibaba Cloud Management Environment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

Service (GPRS) ● Satellite communications		sensitive cardholder data transmission over open, public network. **VPN Gateway:** Customers are responsible for configuring VPN configuration to protect cardholder data transmission over IPsec VPN network if the service is used. **SLB, CDN, SCDN, and DCDN:** SLB, CDN, SCDN, and DCDN are the compliance solutions for customer to meet PCI DSS requirement 4.1. Customers are responsible for configuring security TLS protocols, choosing strong encryption ciphers and using trusted certificates to safeguard sensitive cardholder data transmission over open, public networks.		
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	**Customer**	**All In-Scope Services:** Customers are responsible for management of their networks, including those with wireless connectivity.	N/A	N/A
4.2 Never send unprotected PANs by end- user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.).	**Customer**	**All In-Scope Services:** Customers are responsible for the use of any end-user messaging technologies for transmitting PAN.	N/A	N/A

4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.3 Maintain a Vulnerability Management Program

4.3.1 Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server,**	**All In-Scope Services:** Alibaba Cloud manages anti-virus software for the Alibaba Cloud	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020.

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**Shared**	**Dedicated Host, Elastic HPC and SCC:** Customers are responsible for implementing and managing anti-virus on customer- managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances to meet PCI requirements.	Management Environment and, where appropriate, for identified services.	Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	**Shared**			
5.2 Ensure that all anti-virus mechanisms are maintained as follows: ● Are kept current, ● Perform periodic scans ● Generate audit logs which are retained per PCI DSS Requirement 10.7.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for implementing and managing anti-virus on customer- managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances to meet PCI requirements.	**All In-Scope Services:** Alibaba Cloud manages anti-virus software for the Alibaba Cloud Management Environment and, where appropriate, for identified services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for implementing and managing anti-virus on customer- managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances to meet PCI requirements.	**All In-Scope Services:** Alibaba Cloud manages anti-virus software for the Alibaba Cloud Management Environment and, where appropriate, for identified services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.3.2 Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk	**Shared**	Customers are responsible for maintaining a vulnerability management process in line with PCI DSS requirement. 6.1. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for MongoDB and AnalyticDB for PostgreSQL:** Customers are responsible for managing the security patches of their ECS, ECS Bare Metal Instance,	**All In-Scope Services:** Alibaba Cloud maintains a process to identify security vulnerabilities for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.		Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for MongoDB and AnalyticDB for PostgreSQL instances. **Security Center:** Customers are responsible for reviewing all Security Center Bulletins and ensuring that any recommendations that are applicable to the customer’s environment are reviewed and implemented as necessary if the service is used.		
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for MongoDB and AnalyticDB for PostgreSQL:** Customers are responsible for managing the security patches of their ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple	**All In-Scope Services:** Alibaba Cloud maintains a security patching process for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		Application Server, Dedicated Host, Elastic HPC and SCC, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for MongoDB and AnalyticDB for PostgreSQL instances. **Security Center:** Customers are responsible for reviewing all Alibaba Cloud Security Bulletins and ensuring that any recommendations that are applicable to the customer's environment are reviewed and implemented as necessary.		
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: ● In accordance with PCI DSS (for example, secure authentication and logging) · Based on industry standards and/or best practices. ● Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development standards maintenance, and ensure applications that developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI	**All In-Scope Services:** Alibaba Cloud is responsible for software development standards maintenance and ensure the applications developed and deployed in Alibaba Cloud Management Environment aligned with PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	**Shared**	DSS requirements.		
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: ● Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. ● Code reviews ensure code is developed according to secure coding guidelines · Appropriate corrections are implemented prior to release. ● Code-review results are reviewed and approved by management prior to release. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	**Shared**			

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**Shared**	**All In-Scope Services:** Customers are responsible for any custom configurations that may be created using development criteria that are allowed by the OpenAPI. Changes to Alibaba Cloud service configurations must be subject to customer change control procedures. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development and change control programs maintenance, and ensure applications that developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI DSS requirements.	**All In-Scope Services:** Alibaba Cloud is responsible for software development and change control programs maintenance, and ensure the applications that developed and deployed in Alibaba Cloud Management Environment aligned with PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development and change control programs maintenance, and ensure applications that	**All In-Scope Services:** Alibaba Cloud is responsible for software development and change control programs maintenance, and ensure the applications that developed and deployed in Alibaba Cloud Management Environment aligned with	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN
6.4.2 Separation of duties between development/test and production environments	**Shared**			
6.4.3 Production data (live PANs) are not used for testing or development	**Shared**			

6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	**Shared**	developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI DSS requirements.	PCI DSS requirements.	Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
6.4.5 Change control procedures must include the following:	**Shared**	**All In-Scope Services:** Customers are responsible for any custom configurations that may be created using development criteria that are allowed by the OpenAPI. Changes to Alibaba Cloud service configurations must be subject to customer change control procedures. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development and change control programs maintenance, and ensure applications that developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI DSS requirements.	**All In-Scope Services:** Alibaba Cloud is responsible for software development and change control programs maintenance, and ensure the applications that developed and deployed in Alibaba Cloud Management Environment aligned with PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
6.4.5.1 Documentation of impact.	**Shared**			
6.4.5.2 Documented change approval by authorized parties.	**Shared**			
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**Shared**			
6.4.5.4 Back-out procedures.	**Shared**			
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	**Shared**			
6.5 Address common coding vulnerabilities in software-	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple**	**All In-Scope Services:** Alibaba Cloud is responsible for software	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by

development processes as follows: ● Train developers at least annually in up- to-date secure coding techniques, including how to avoid common coding vulnerabilities. ● Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.		**Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development and change control programs maintenance, and ensure applications that developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI DSS requirements.	development and change control programs maintenance，and ensure the applications that developed and deployed in Alibaba Cloud Management Environment aligned with PCI DSS requirements.	atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
Note: Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).				
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for software development and change control programs maintenance, and ensure applications that developed and deployed on ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances aligned with PCI	**All In-Scope Services:** Alibaba Cloud is responsible for software development and change control programs maintenance，and ensure the applications that developed and deployed in Alibaba Cloud Management Environment aligned with PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
6.5.2 Buffer overflows	**Shared**			
6.5.3 Insecure cryptographic storage	**Shared**			
6.5.4 Insecure communications	**Shared**			
6.5.5 Improper error handling	**Shared**			
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	**Shared**			
6.5.7 Cross-site scripting (XSS)	**Shared**			

6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	**Shared**	DSS requirements.		
6.5.9 Cross-site request forgery (CSRF)	**Shared**			
6.5.10 Broken authentication and session management.	**Shared**			
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ● Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. ● Installing an automated technical solution that detects and prevents web- based attacks (for example, a web- application firewall) in front of public- facing web applications, to continually check all traffic.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for Web Application Filtering or application security reviews for web applications deployed on customer-managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances. **WAF:** WAF is one of the compliance solution for customer to meet PCI DSS requirement 6.6. It's customers' responsible for deploying and configuring WAF for web applications deployed on customer-managed ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances.	**All In-Scope Services:** Alibaba Cloud is responsible for Web Application Filtering or application security reviews for web applications deployed in the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.4 Implement Strong Access Control Measures

4.4.1 Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**Shared**	**All In-Scope Services:** Customers are responsible for managing access to all Alibaba Cloud services that	**All In-Scope Services:** Alibaba Cloud maintains the access controls related to underlying	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020.

7.1.1 Define access needs for each role, including: · System components and data resources that each role needs to access for their job function · Level of privilege required (for example, user, administrator, etc.) for accessing resources.	**Shared**	are included in their CDE. Alibaba Cloud provides various mechanisms for controlling access to the services including RAM with granular access controls to the Alibaba Cloud Management Console and cloud service, and IDaaS for application centralized identity, permissions, and application management services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for access control within all ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirement 7.1.2 for the purchased cloud service and customer application. Customers are responsible for implementing and configuring RAM and / or IDaaS to restrict access privileged user IDs to least privileges necessary to perform job responsibilities	infrastructure systems and the Alibaba Cloud Management Environment.	Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	**Shared**			
7.1.3 Assign access based on individual personnel's job classification and function.	**Shared**			
7.1.4 Require documented approval by authorized parties specifying required privileges.	**Shared**			

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:				
7.2.1 Coverage of all system components	**Shared**	**All In-Scope Services:** Customers are responsible for managing access to all Alibaba Cloud services that are included in their CDE. Alibaba Cloud provides various mechanisms for controlling access to the services including RAM with granular access controls to the Alibaba Cloud Management Console. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for access control within all ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirement 7.2 for the purchased cloud service and customer application. Customers are responsible	**All In-Scope Services:** Alibaba Cloud maintains the access controls related to underlying infrastructure systems and the Alibaba Cloud Management Environment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
7.2.2 Assignment of privileges to individuals based on job classification and function.	**Shared**			
7.2.3 Default "deny-all" setting.	**Shared**			

		for implementing and configuring RAM and / or IDaaS to restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed		
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.4.2 Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders).

However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of- sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts to align with the applicable PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirements 8.1.1, 8.1.2, 8.1.3, 8.1.4 and 8.1.5 for the purchased cloud service and customer application. Customers are responsible for implementing, configuring and managing RAM and / or IDaaS to ensure proper user identification management.	**All In-Scope Services:** Alibaba Cloud is responsible for providing each user in the Alibaba Cloud Management Environment with a unique ID. Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with these PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS provide security functions for Alibaba Cloud customers to further protect their accounts and control access, such features as multi-factor authentication, strong password policies, and separation of console users from API users, custom fine-grained	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**Shared**			
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Shared**			
8.1.3 Immediately revoke access for any terminated users.	**Shared**			
8.1.4 Remove/disable inactive user accounts within 90 days.	**Shared**			
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use.	**Shared**			

			authorization policies, grouped authorization, temporary authorization token and account temporary suspension.	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts to align with the applicable PCI DSS requirements. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for establishing a policy for the ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances that align with the applicable PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirements 8.1.6, 8.1.7 and 8.1.8 for the purchased cloud service and customer application. Customers are responsible for implementing, configuring and managing RAM and / or IDaaS to ensure proper user	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with these PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS provide security functions for Alibaba Cloud customers to further protect their account and control access, such features as multi-factor authentication, strong password policies, and separation of console users from API users, custom fine-grained authorization policies, grouped authorization, temporary authorization token and account temporary suspension.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**Shared**			
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**Shared**			

		identification management.		
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: ● Something you know, such as a password or passphrase ● Something you have, such as a token device or smart card ● Something you are, such as a biometric.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts, including Alibaba Cloud accounts. This includes access controls to all in scope Alibaba Cloud Services as well as to the server instances and applications that customers may be hosting on ECS server instances.	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts to align with this PCI DSS requirement. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** customers are responsible for the processes and creation of accounts and access controls using the various authentication mechanisms offered by Alibaba Cloud. This includes access controls to all Alibaba Cloud Services	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with this PCI DSS requirement. **RAM and IDaaS:** RAM and IDaaS provide security functions for Alibaba Cloud customers to further protect their account and control access, such features as multi-factor authentication, strong password policies, and separation of console users from API users,	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		included in scope as well as to the server instances and applications that customers may be hosting in ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC. Customers are responsible for ensuring proper configuration of the authentication mechanisms to ensure that passwords are unreadable in storage and transmission. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirement 8.2.1 for the purchased cloud service and customer application. Customers are responsible for implementing, configuring and managing RAM and / or IDaaS to ensure all authentication credentials unreadable during transmission and storage on all system components	custom fine-grained authorization policies, grouped authorization, temporary authorization token and account temporary suspension.	
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts, including Alibaba Cloud accounts. This includes access controls to all in scope Alibaba Cloud Services as well as to the server instances and applications	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with this PCI DSS requirement.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for

		that customers may be hosting on ECS server instances.		Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.2.3 Passwords/passphrases must meet the following: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts to align with the applicable PCI DSS requirements. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for establishing a policy for the OS of ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances that align with the applicable PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS are the compliance solutions for customer to meet PCI DSS requirements 8.2.3, 8.2.4, 8.2.5 and 8.2.6 for the purchased cloud service and customer application. Customers are responsible for implementing, configuring and managing	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with these PCI DSS requirements. **RAM and IDaaS:** RAM and IDaaS provide security functions for Alibaba Cloud customers to further protect their account and control access, such features as multi-factor authentication, strong password policies, and separation of console users from API users, custom fine-grained authorization policies, grouped authorization, temporary authorization token and account	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.2.4 Change user passwords/passphrases at least once every 90 days.	**Shared**			
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	**Shared**			
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	**Shared**			

		RAM and / or IDaaS password policies to meet PCI DSS requirements		
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.				
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	**Shared**	**All In-Scope Services:** Customers are responsible for the management consoles, OpenAPI and any other in scoped authentication mechanisms management. Alibaba Cloud RAM, IDaaS and VPN Gateway provide an opt-in Multi-Factor authentication solution to support customers meeting the PCI DSS requirement. **RAM, IDaaS and VPN Gateway:** RAM, IDaaS and VPN Gateway are the compliance solutions for customer to meet PCI DSS requirements 8.3.1 and 8.3.2 for the purchased cloud service, customer application and environment. Customers are responsible for implementing, configuring	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with these PCI DSS requirements. **RAM, IDaaS VPN Gateway:** RAM, IDaaS and VPN Gateway provide multi-factor authentication security functions for Alibaba Cloud customers to further protect their accounts or remote network access to customers' CDE	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.				

		and managing RAM, IDaaS and VPN Gateway to meet PCI DSS requirements.		
8.4 Document and communicate authentication policies and procedures to all users including: ● Guidance on selecting strong authentication credentials ● Guidance for how users should protect their authentication credentials ● Instructions not to reuse previously used passwords ● Instructions to change passwords if there is any suspicion the password could be compromised.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that their policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ● Generic user IDs are disabled or removed. ● Shared user IDs do not exist for system administration and other critical functions. ● Shared and generic user IDs are not used to administer any system components.	**Shared**	**All In-Scope Services:** Customers are responsible for managing the creation of user accounts to align with this PCI DSS requirement. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that their policies and procedures are documented and known to all affected parties. Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020

8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.	**Shared**	are responsible for establishing a policy for the ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances that align with the applicable PCI DSS requirements.	account and control access to align with these PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: ● Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. ● Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**Shared**	**All In-Scope Services:** Customers are responsible for the management consoles and OpenAPI authentication mechanisms management. Alibaba Cloud RAM provides an opt-in Multi-Factor Authentication (MFA) solution to support customers meeting the PCI DSS requirement.	**All In-Scope Services:** Alibaba Cloud is responsible for providing security functions for Alibaba Cloud customers to further protect their account and control access to align with these PCI DSS requirements.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: ● All user access to, user queries of, and user actions on databases are through programmatic methods. ● Only database administrators have the ability to directly access	**Customer**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for managing the creation of user accounts. This includes access controls to all applications installed by	N/A	N/A

or query databases. ● Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).		the customer, including databases. **ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcached**: customers are responsible for managing the creation of user accounts with access to databases		
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.4.3 Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A

"visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the physical security for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of- sale terminals are present, such as the cashier areas in a retail store.	**Alibaba Cloud**			
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network	**Alibaba Cloud**			

jacks.				
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**Alibaba Cloud**			
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: ● Identifying onsite personnel and visitors (for example, assigning badges) ● Changes to access requirements ● Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the physical security for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.3 Control physical access for onsite personnel to sensitive areas as follows: ● Access must be authorized and based on individual job function. ● Access is revoked immediately upon termination, and all physical access mechanisms, such as	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the physical security for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020.

keys, access cards, etc., are returned or disabled.				Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:				
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the physical security for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	**Alibaba Cloud**			
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	**Alibaba Cloud**			
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**Alibaba Cloud**			

9.5 Physically secure all media.	**Shared**	**All In-Scope Services:** Customers are responsible for backup, compliance with PCI DSS requirements outside of the Alibaba Cloud environment.	**All In-Scope Services:** Alibaba Cloud maintains the media handling controls for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	**Shared**			
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**Shared**	**All In-Scope Services:** Customers are responsible for backup, compliance with PCI DSS requirements outside of the Alibaba Cloud environment.	**All In-Scope Services:** Alibaba Cloud maintains the media handling controls for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.6.1 Classify media so the sensitivity of the data can be determined.	**Shared**			
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**Shared**			
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	**Shared**			
9.7 Maintain strict control over the storage and accessibility of media.	**Shared**	**All In-Scope Services:** Customers are responsible for backup, compliance with PCI DSS requirements outside of the Alibaba	**All In-Scope Services:** Alibaba Cloud maintains the media handling controls for Alibaba Cloud data centers and co-locations supporting	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for
9.7.1 Properly maintain inventory logs of all media and conduct media	**Shared**			

inventories at least annually.		Cloud environment.	the services included in the PCI DSS assessment.	Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	**Shared**	**All In-Scope Services:** Customers are responsible destruction of media outside of the Alibaba Cloud environment.	**All In-Scope Services:** Alibaba Cloud maintains the media handling controls for Alibaba Cloud data centers and co-locations supporting the services included in the PCI DSS assessment.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	**Shared**			
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**Shared**			
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. Note: These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS	**Customer**	**All In-Scope Services:** Customers are responsible for all devices management that capture payment card data via direct physical interaction with the card.	N/A	N/A

keypads.				
9.9.1 Maintain an up-to-date list of devices. The list should include the following: ● Make, model of device ● Location of device (for example, the address of the site or facility where the device is located) ● Device serial number or other method of unique identification.	**Customer**	**All In-Scope Services:** Customers are responsible for all devices management that capture payment card data via direct physical interaction with the card.	N/A	N/A
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.	**Customer**	**All In-Scope Services:** Customers are responsible for all devices management that capture payment card data via direct physical interaction with the card.	N/A	N/A
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: ● Verify the identity of any third-	**Customer**	**All In-Scope Services:** Customers are responsible for providing training to ensure appropriate personnel are aware of any tampering or	N/A	N/A

party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Do not install, replace, or return devices without verification. ● Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).		replacement of point-of-sale devices or abnormalities of point-of-sale locations.		
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.5 Regularly Monitor and Test Networks

4.5.1 Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
10.1 Implement audit trails to link all access to system components to each individual user.	**Shared**	**All In-Scope Services:** Customers are responsible for implementing audit trails system or mechanism to link all access to purchased cloud service. **ActionTrail:** ActionTrail is one of the compliance solution for customer to access Alibaba Cloud Console and all command-line of OpenAPI actions log. Customer are responsible for enable and configuring the ActionTrail to record the Alibaba Cloud Console and OpenAPI action log. **Bastionhost:** Bastionhost is one of the compliance solution for customer to maintain audit logs for ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC to meet PCI DSS requirement	**All In-Scope Services:** Alibaba Cloud maintains and monitors audit logs for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		10.1, . Customer are responsible for enable and configuring the Bastionhost to link all access to the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC OS. **DBAudit:** DBAudit is one of the compliance solution for customer to maintain audit logs for ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcacher. Customer are responsible for enable and configuring the DBAudit and purchased ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcacher service to record the audit logs for customers		
10.2 Implement automated audit trails for all system components to				

reconstruct the following events:				
10.2.1 All individual user accesses to cardholder data	**Shared**	**All In-Scope Services:** Customers are responsible for configuring logging parameters, when available. **ActionTrail:** ActionTrail is one of the compliance solution for customer to access Alibaba Cloud Console and all command-line of OpenAPI actions log. Customer are responsible for enable and configuring the ActionTrail to record the Alibaba Cloud Console and OpenAPI action log. **Bastionhost:** Bastionhost is one of the compliance solution for customer to maintain audit logs for ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC to meet PCI DSS requirement 10.1, . Customer are responsible for enable and configuring the Bastionhost to link all access to the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC OS. **DBAudit:** DBAudit is one of the compliance solution	**All In-Scope Services:** Alibaba Cloud maintains and monitors audit logs for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
10.2.2 All actions taken by any individual with root or administrative privileges	**Shared**			
10.2.3 Access to all audit trails	**Shared**			
10.2.4 Invalid logical access attempts	**Shared**			
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	**Shared**			
10.2.6 Initialization, stopping, or pausing of the audit logs	**Shared**			
10.2.7 Creation and deletion of system- level objects	**Shared**			

		for customer to maintain audit logs for ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcacher. Customer are responsible for enable and configuring the DBAudit and purchased ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ApsaraDB for Memcacher service to record the audit logs for customers		
10.3 Record at least the following audit trail entries for all system components for each event:				
10.3.1 User identification	**Shared**	**All In-Scope Services:** Customers are responsible for configuring logging parameters, when available. **ActionTrail:** ActionTrail is one of the compliance solution for customer to access Alibaba Cloud Console and all command-line of OpenAPI actions log.	**All In-Scope Services:** Alibaba Cloud maintains and monitors audit logs for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on
10.3.2 Type of event	**Shared**			
10.3.3 Date and time	**Shared**			
10.3.4 Success or failure indication	**Shared**			
10.3.5 Origination of event	**Shared**			
10.3.6 Identity or name of affected data, system component, or resource.	**Shared**			

		Customer are responsible for enable and configuring the ActionTrail to record the Alibaba Cloud Console and OpenAPI action log. **Bastionhost:** Bastionhost is one of the compliance solution for customer to maintain audit logs for ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC to meet PCI DSS requirement 10.1, . Customer are responsible for enable and configuring the Bastionhost to link all access to the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC OS. **DBAudit:** DBAudit is one of the compliance solution for customer to maintain audit logs for ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher. Customer are responsible for enable and configuring the DBAudit and purchased		September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher service to record the audit logs for customers		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for appropriately managing time service (NTP) configuration for the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances.	**All In-Scope Services:** Alibaba Cloud is responsible for managing time service (NTP) configuration for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
10.4.1 Critical systems have the correct and consistent time.	**Shared**			
10.4.2 Time data is protected.	**Shared**			
10.4.3 Time settings are received from industry-accepted time sources.	**Shared**			
10.5 Secure audit trails so they cannot be altered.	**Shared**	**All In-Scope Services:** Customers are responsible for setting permissions and access controls for the audit logs of purchased cloud services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic**	**All In-Scope Services:** Alibaba Cloud is responsible for audit trails management for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on
10.5.1 Limit viewing of audit trails to those with a job-related need.	**Shared**			
10.5.2 Protect audit trail files from unauthorized modifications.	**Shared**			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**Shared**			

10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	**Shared**	**HPC and SCC:** Customers are responsible for protecting, configuring and monitoring the audit logs on the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instances or forward the logs to centralized log solution in alignment with PCI DSS requirements. **OSS, ActionTrail and Log Service:** OSS, Action Trail and Log Service are the solutions for customers to maintain the audit logs. If OSS, ActionTrail or Log Service is used, customers are responsible for setting permissions and access controls for audit logs in OSS, ActionTrail and Log Service.		September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**Shared**			
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.				

10.6.1 Review the following at least daily: · All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**Shared**	**All In-Scope Services:** Customers are responsible for all logs review and process(including but not limited to action logs of Alibaba Cloud Console and OpenAPI, audit logs of ECS OS, Database operation logs, etc.) and security events generated by the purchased cloud services.	**All In-Scope Services:** Alibaba Cloud is responsible for managing/ reviewing logs and security events for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	**Shared**			
10.6.3 Follow up exceptions and anomalies identified during the review process.	**Shared**			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**Shared**	**All In-Scope Services:** Customers are responsible for retention of all logs (including but not limited to action logs of Alibaba Cloud Console and OpenAPI, audit logs of ECS OS, Database operation logs, etc.) in alignment with PCI DSS requirements. **OSS, and ActionTrail:** OSS and Action Trail are the compliance solutions	**All In-Scope Services:** Alibaba Cloud is responsible for obtaining and retaining audit trail for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for

		for customers to maintain the audit logs to meet PCI DSS requirement 10.7. If OSS or ActionTrail is used, customers are responsible for configuring OSS and ActionTrail retention cycle to meet PCI DSS requirement. **Log Service:** Log Service is one of the compliance solution for customer to maintain audit logs for ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, Alibaba Cloud Container Service for Kubernetes, MaxCompute, OSS, Apsara File Storage NAS, Anti-DDoS Basic, Anti-DDoS Pro, Anti-DDoS Premium, WAF, Security Center, Cloud Firewall, DBAudit, SLB, VPC, Elastic IP Address, CDN, DCDN, SCDN, BastionHost, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis and ApsaraDB for MongoDB to meet PCI DSS requirement 10.7. Customer are responsible for enable and configuring the Log Service and purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application		Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

		Server, Dedicated Host, Elastic HPC, SCC, Alibaba Cloud Container Service for Kubernetes, MaxCompute, OSS, Apsara File Storage NAS, Anti-DDoS Basic, Anti-DDoS Pro, Anti-DDoS Premium, WAF, Security Center, Cloud Firewall, DBAudit, SLB, VPC, Elastic IP Address, CDN, DCDN, SCDN, BastionHost, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis and ApsaraDB for MongoDB service to record the action log for customers.		
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: ● *Firewalls* ● *IDS/IPS* ● *FIM* ● *Anti-virus* ● *Physical access controls* ● *Logical access controls* ● *Audit logging mechanisms* ● *Segmentation controls (if used)*	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring a process is implemented for timely response to any critical security control failures.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring a process is implemented for timely response to any critical security control failures for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: ● *Restoring security functions · Identifying and documenting the duration (date and time start to end) of the security failure* ● *Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause* ● *Identifying and addressing any security issues that arose during the failure* ● *Performing a risk assessment to determine whether further actions are required as a result of the security failure* ● *Implementing controls to prevent cause of failure from reoccurring* ● *Resuming monitoring of security controls*	**Shared**			
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020

				Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.5.2 Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the processes to conduct rogue wireless access point detection for Alibaba Cloud data centers.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the processes to conduct rogue wireless access point detection for Alibaba Cloud data	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for

			centers.	Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	**Alibaba Cloud**	N/A	**All In-Scope Services:** Alibaba Cloud maintains the response procedures in the event unauthorized wireless access points are detected for Alibaba Cloud data centers.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable				

vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.				
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud Container Service for Kubernetes and Elasticsearch:** Customers are responsible for external	**All In-Scope Services:** Alibaba Cloud manages vulnerability scan for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide	**Shared**			

published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.		ASV scan and internal vulnerability scan for the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud Container Service for Kubernetes and Elasticsearch instances and applications deployed by the customers. Scans should include customer IP addresses and not Alibaba Cloud endpoints. Alibaba Cloud endpoints are tested as part of Alibaba Cloud vulnerability scans.		
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**Shared**			

11.3 Implement a methodology for penetration testing that includes the following: ● Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) ● Includes coverage for the entire CDE perimeter and critical systems ● Includes testing from both inside and outside the network ● Includes testing to validate any segmentation and scope-reduction controls ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 ● Defines network-layer penetration tests to include components that support network functions as well as operating systems ● Includes review and consideration of threats and vulnerabilities experienced in the last 12 months ● Specifies retention of penetration testing results and remediation activities results.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud Container Service for Kubernetes and Elasticsearch:** Customers are responsible for external and internal Penetration Testing for the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud	**All In-Scope Services:** Alibaba Cloud manages Penetration Testing for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**Shared**			

11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**Shared**	Container Service for Kubernetes and Elasticsearch instances and applications deployed by the customers. Penetration Testing should include customer IP addresses and not Alibaba Cloud endpoints. Alibaba Cloud endpoints are tested as part of Alibaba Cloud Penetration Testing.		
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	**Shared**			
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud Container Service for Kubernetes and Elasticsearch:** Customers are responsible for external and internal Penetration Testing on segmentation controls at least every six months and after any	**All In-Scope Services:** Alibaba Cloud manages Penetration Testing for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	**Shared**			

		changes to segmentation controls/methods for the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC, ApsaraDB for PolarDB, DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB, ApsaraDB for Memcacher BastionHost, DBAudit, Alibaba Cloud Container Service for Kubernetes and Elasticsearch instances and applications deployed by the customers. Penetration Testing should include customer IP addresses and not Alibaba Cloud endpoints. Alibaba Cloud endpoints are tested as part of Alibaba Cloud Penetration Testing.		
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for implementing IDS or HIDS functionality for network	**All In-Scope Services:** Alibaba Cloud implements and monitors IDS/IPS on networks that implement Alibaba Cloud services.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020.

prevention engines, baselines, and signatures up to date.		segments they implement and manage. **Security Center:** Customers are responsible for implementing and managing the Security Center agent on customer-managed OS (including but not limited to ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC instance) if the service is used.		Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (Continued on next page) Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the	**Shared**	**ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** Customers are responsible for file integrity monitoring for the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC instances and applications deployed by the customers.	**All In-Scope Services:** Alibaba Cloud manages file integrity monitoring for the Alibaba Cloud Management Environment and Alibaba Cloud service infrastructure.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

merchant or service provider).				
11.5.1 Implement a process to respond to any alerts generated by the change- detection solution.	**Shared**			
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	**Shared**	**All In-Scope Services:** Customers are responsible for ensuring that their policies and procedures are documented and known to all affected parties.	**All In-Scope Services:** Alibaba Cloud is responsible for ensuring that its policies and procedures are documented and known to all affected parties.	Attestation of Compliance for Alibaba Cloud Public Cloud International Services issued by atsec on July 28, 2020. Attestation of Compliance for Alibaba Cloud Security Services issued by atsec on August 5, 2020. Attestation of Compliance for Alibaba Cloud CDN and DCDN Service issued by atsec on September 10, 2020 Attestation of Compliance for Alibaba Cloud Aliyun Fincloud issued by atsec on December 2, 2020.

4.6 Maintain an Information Security Policy

4.6.1 Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
12.1 Establish, publish, maintain, and disseminate a security policy.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A

12.2 Implement a risk-assessment process that: ● Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), ● Identifies critical assets, threats, and vulnerabilities, and ● Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.3.1 Explicit approval by authorized parties	**Customer**			
12.3.2 Authentication for use of the technology	**Customer**			
12.3.3 A list of all such devices and personnel with access	**Customer**			
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example,	**Customer**			

labeling, coding, and/or inventorying of devices)				
12.3.5 Acceptable uses of the technology	**Customer**			
12.3.6 Acceptable network locations for the technologies	**Customer**			
12.3.7 List of company-approved products	**Customer**			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**Customer**			
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**Customer**			
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	**Customer**			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable	N/A	N/A

12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: ● *Overall accountability for maintaining PCI DSS compliance* ● *Defining a charter for a PCI DSS compliance program and communication to executive management*	**Customer**	to their cardholder data environment to maintain compliance with the PCI DSS.		
12.5 Assign to an individual or team the following information security management responsibilities:	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.5.1 Establish, document, and distribute security policies and procedures.	**Customer**			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**Customer**			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**Customer**			
12.5.4 Administer user accounts, including additions, deletions, and modifications.	**Customer**			
12.5.5 Monitor and control all access to data.	**Customer**			
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable	N/A	N/A

12.6.1 Educate personnel upon hire and at least annually. *Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	**Customer**	to their cardholder data environment to maintain compliance with the PCI DSS.		
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**Customer**			
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.8.1 Maintain a list of service providers including a description of the service provided.	**Customer**			

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	**Customer**			
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**Customer**			
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**Customer**			
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**Customer**			

12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	**Customer**	**All In-Scope Services:** Customers are responsible for maintaining policies and processes applicable to their cardholder data environment to maintain compliance with the PCI DSS.	N/A	N/A
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**Customer**	**All In-Scope Services:** Customers are responsible for policies and processes maintenance and ensure the policies and processes compliance with the PCI DSS requirements.	N/A	N/A
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ● Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ● Specific incident response procedures ● Business recovery and continuity procedures ● Data backup processes	**Customer**			

• Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.				
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	**Customer**			
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**Customer**			
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	**Customer**			
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**Customer**			
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**Customer**			

12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: ● *Daily log reviews* ● *Firewall rule-set reviews* ● *Applying configuration standards to new systems* ● *Responding to security alerts* ● *Change management processes*	**Customer**	**All In-Scope Services:** Customers are responsible for policies and processes maintenance and ensure the policies and processes compliance with the PCI DSS requirements.	N/A	N/A
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: ● Documenting results of the reviews ● Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	**Customer**			

4.7 Additional PCI DSS Requirements

4.7.1 Additional PCI DSS Requirements for Shared Hosting Providers

As referenced in Requirement 12.8 and 12.9, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.	**Customer**	**All In-Scope Services:** Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. Customers are responsible for protecting their customer's data within Alibaba Cloud services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** The Secondary Shared-Hosting Provider is responsible for entities' hosted environments and ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC instances protection.	N/A	N/A
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**Customer**			
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**Customer**			
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**Customer**			
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**Customer**	**All In-Scope Services:** Customers may also be considered a shared hosting provider, if they run applications or store data for their customers.	**N/A**	N/A

		Customers are responsible for protecting their customer's data within Alibaba Cloud services. **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC:** The Secondary Shared-Hosting Provider is responsible for entities' hosted environments and ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC, SCC instances protection.		

4.7.2 Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

Entities using SSL and early TLS for POS POI terminal connections must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment terminals. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS must not be used as a security control to meet these requirements, except in the case of POS POI terminal connections as detailed in this appendix. To support entities working to migrate away from SSL/early TLS on POS POI terminals, the following provisions are included:

New POS POI terminal implementations must not use SSL or early TLS as a security control.

All POS POI terminal service providers must provide a secure service offering.

Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.

POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, **and the SSL/TLS termination points to which they connect,** may continue using SSL/early TLS as a security control.

This Appendix only applies to entities using SSL/early TLS as a security control to protect POS POI terminals, including service providers who provide connections into POS POI terminals.

PCI DSS Requirements	Responsibility	Scope of Customer PCI DSS Responsibility	Scope of Alibaba Cloud PCI DSS Responsibility	Evidence of Alibaba Cloud Demonstrating Its PCI DSS Compliance
A2.1 Where POS POI terminals (at the merchant or payment acceptance location) use SSL and/or early TLS, the entity must confirm the devices are not susceptible to any known exploits for those protocols. Note: This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.	**Customer**	**All In-Scope Services:** Customers are responsible for using TLS 1.1 protocol or higher. If early versions of TLS 1.1 or SSL protocol are in place in the cardholder data environment, Customers are responsible for developing a compensating control to mitigate the security risk.	N/A	N/A

A2.2 *Requirement for Service Providers Only:* All service providers with existing connection points to POS POI terminals referred to in A2.1 that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	**Customer**	**All In-Scope Services:** Customers are responsible for using TLS 1.1 protocol or higher. If early versions of TLS 1.1 or SSL protocol are in place in the cardholder data environment, Customers are responsible for developing a compensating control to mitigate the security risk.	N/A	N/A
A2.3 *Requirement for Service Providers Only:* All service providers must provide a secure service offering.	**Customer**	**All In-Scope Services:** Customers are responsible for using TLS 1.1 protocol or higher. If early versions of TLS 1.1 or SSL protocol are in place in the cardholder data environment, Customers are responsible for developing a compensating control to mitigate the security risk.	N/A	N/A

5 Customer PCI DSS Compliance Implementation Considerations

As Alibaba Cloud customers leverage Alibaba Cloud to implement a compliant cardholder environment, there are a number of considerations for Alibaba Cloud customers, as a service provider or merchant, when implementing a cardholder environment. The information below provides some considerations and should be read in combination with the chapter 4 “PCI DSS Requirements and Responsiblity Management Matrix Of Alibaba Cloud“.

- **Choose Service Locations**

  Alibaba Cloud's data centers are deployed across multiple regions worldwide, with each region supporting multiple zones. Customer businesses can be deployed across regions and zones to implement a high availability architecture. The PCI DSS validated data centers should be considered when customers implementing its PCI DSS compliance.

- **ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC Operating System Hardened**

  Alibaba Cloud does provide images that can be used for deployment of host operating systems, Alibaba Cloud customers need to develop and implement system configuration and hardening standards to align with all applicable PCI DSS 2.2, 2.2.1-2.2.5, 2.3, 8.1.6-8.1.8, 8.2.1, 8.2.3-8.2.5 requirements for operating systems. Alibaba Cloud customers own and manage their own instance operating system and the images provided are not intended to represent a PCI compliant platform.

- **ECS Image Hardened**

  An image is an execution environment template for ECS virtual machine instances. It generally includes an operating system and preinstalled software. Alibaba Cloud ECS tenants can use an image to create an ECS instance or make changes to the system disk of an ECS instance. The security hardening of Alibaba Cloud public image (supports various Linux/Windows release versions) contains three parts: image security configuration, image vulnerability repair, and default security software in an image. Alibaba Cloud monitors the vulnerabilities in Alibaba Cloud public image operating systems and third-party software in real time to ensure that all high-risk vulnerabilities in Alibaba Cloud public images are repaired in a timely manner. Alibaba Cloud public images are configured with security best practices for the virtual machine by default. Besides, all Alibaba Cloud public images includes Alibaba Cloud Security Center agent by default to guarantee the security of instances upon boot up. However the tenants need to development and implement system configuration and hardening standards for ECS image to align with all applicable PCI DSS 2.2, 2.2.1-2.2.5, 2.3, 8.1.6-8.1.8, 8.2.1, 8.2.3-8.2.5 requirements.

- **Cloud Firewall**

  Cloud Firewall is Firewall as a Service (FWaaS) solution that is provided by Alibaba Cloud for public clouds. Cloud Firewall allows customers to centrally manage the access control policies that are used to control traffic from the Internet to the ECS instances and the micro segmentation policies that are used to control traffic between ECS instances. With Cloud Firewall, customers can protect traffic from public IP addresses of ECS, Elastic IP addresses (EIPs) of SLB, some public IP addresses of SLB, high-availability virtual IP addresses (HAVIP), EIPs, EIPs of ECS, EIPs of Elastic Network Interface (ENI), and EIPs of NAT Gateway and traffic between VPCs that are connected by using a CEN

or Express Connect. If Cloud firewall is used as PCI DSS solution by customers, it is the customers' responsibility for utilizing the Cloud Firewall in a manner that maintains compliance with PCI DSS 1.2, 1.2.1-1.2.3, 1.3, 1.3.1-1.3.7 requirements to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

- **VPC**

  Customers have full control of the VPC instances provided by Alibaba Cloud. With VPC, customers can build an isolated network environment and customize IP address ranges, network segments, routing tables, and gateway. In addition, user can use connection methods like physical connection and VPN to connect VPCs with traditional IDCs, and thus build a hybrid cloud service. Customers should align with all applicable PCI DSS 1.2, 1.2.1-1.2.3, 1.3, 1.3.1-1.3.7 requirements to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

- **Security group**

  Security group offers the capability of distributed virtual firewall. A security group is a logical group that consists of instances with the same security requirements and mutual trust in the same region. Security groups are used to set network access control for one or more ECS server instances. It is an important network security isolation tool and is used to divide network security domains on the cloud. If Security group is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the security group in a manner that maintains compliance with PCI DSS 1.2, 1.2.1-1.2.3, 1.3, 1.3.1-1.3.7 requirements to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

- **VPN Gateway**

  VPN Gateway (Virtual Private Network Gateway) is an Internet-based service that establishes a secure and reliable connection among on-premise data centers, office networks, and Alibaba Cloud VPC over encrypted channels. If VPN is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the VPN service in a manner that maintains compliance with PCI DSS 8.3.2 requirements to provide Multi-Factor authentication for remote access to customers' CDE.

- **SLB**

  Alibaba Cloud SLB is a ready-to-use service that seamlessly integrates with ECS. It is a load balancing service that distributes varying traffic levels among multiple backend ECS server instances without manual intervention. SLB ensures high availability by eliminating single point of failure, and protects against SYN flood and DDoS attacks. SLB provides a certificate management system where user certificates and keys are managed and stored. Private keys uploaded to the certificate management system will be stored encrypted. If SLB is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the SLB service in a manner that maintains compliance with PCI DSS 4.1 requirement to choose TLS protocols, encryption ciphers to safeguard sensitive cardholder data transmission over open, public networks.

- **NAT Gateway**

  NAT Gateway is an enterprise-class VPC Internet gateway that provides NAT proxy services (SNAT and DNAT) for customers. SNAT allows an ECS instance without a public IP address to access the Internet. DNAT maps a public IP address of a NAT Gateway to an ECS instance so

that the ECS instance can be accessible from the Internet. As an Internet gateway, a NAT Gateway requires public IP addresses to function. After creating a NAT Gateway, customers can associate one or more Elastic IP Addresses (EIPs) with the NAT Gateway. If NAT Gateway is used as PCI DSS solution by customers, it is the customers' responsibility for utilizings the NAT Gateway in a manner that maintains compliance with PCI DSS 1.3.7 requirements to prevent the disclosure of IP addresses and routing information for CDE.

- **RAM**

  RAM service is provided for user identity management and resource access control. RAM enables an Alibaba Cloud account to have multiple independent subusers. It also supports such features as multi-factor authentication, strong password policies, separation of console users from API users, custom fine-grained authorization policies, grouped authorization, temporary authorization token and account temporary suspension. If RAM is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the RAM service in a manner that maintains compliance with PCI DSS 8.1.1-8.1.8, 8.2.1, 8.2.3-8.2.5, 8.3.1 requirements to ensure proper user identification management, protect all authentication credentials unreadable during transmission and storage on all system components, guarantee strong password policies and provide multi-factor authentication for customers.

- **Identity as a service (IDaaS)**

  Alibaba Cloud Identity as a Service (IDaaS) is a set of centralized identity, permission, and application management services provided by Alibaba Cloud for enterprise users to help customers integrate and deploy all the identities of the internal office system, business system and the three-party SaaS system realize one account to open up all application services locally or in the cloud. If IDaaS is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the RAM service in a manner that maintains compliance with PCI DSS 8.1.1-8.1.8, 8.2.1, 8.2.3-8.2.5, 8.3.1 requirements to ensure proper user identification management, protect all authentication credentials unreadable during transmission and storage on all system components, guarantee strong password policies and provide multi-factor authentication for customers.

- **Data Encryption Service**

  Alibaba Cloud customers retain the responsibility for transport and storage encryption of cardholder data for their environment. Data Encryption Service Encryption service uses hardware encryption machines that have been tested and certified by the National Cryptographic Administration as a service. If Data Encryption Service is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the Data Encryption Service in a manner that maintains compliance with PCI DSS 3.4, 3.6.1 and 3.6.8 requirements to protect CHD and the keys used for CHD protection.

- **KMS**

  Alibaba Cloud customers retain the responsibility for transport and storage encryption of cardholder data for their environment.KSM provides secure and compliant key management and cryptography services to help customers encrypt and protect sensitive data assets. If KMS is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the KMS service in a manner that maintains compliance with PCI DSS 3.4, 3.6.1 and 3.6.8 requirements to protect CHD and the keys used for CHD protection.

- **BastionHost**

Bastionhost enables customers to manage asset O&M permissions in a centralized manner, monitor all O&M operations, and reproduce O&M scenarios in real time to facilitate identity authentication, access control, and operation audit. If Bastionhost is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the Bastionhost service in a manner that maintains compliance with PCI DSS 10.1 requirement to link all access to the purchased ECS, ECS Bare Metal Instance, Elastic GPU Service, Simple Application Server, Dedicated Host, Elastic HPC and SCC OS.

- **DBAudit**

  DBAudit is a professional, active, and real-time database security audit service that can be used to audit DRDS, PolarDB-X, ApsaraDB RDS for MySQL, ApsaraDB RDS for PostgreSQL, ApsaraDB for MariaDB TX, ApsaraDB RDS for PPAS, ApsaraDB for Redis, ApsaraDB for MongoDB and ECS self-built database in the Alibaba Cloud environment. If DBAudit is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the DBAudit service in a manner that maintains compliance with PCI DSS 10.1, 10.2 and 10.3 requirements to record the database audit logs for customers.

- **Log Service**

  Log Service supports collection, consumption, shipping, search, and analysis of logs, and improves the capacity of processing and analyzing large amounts of logs. If Log Service is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the Log Service in a manner that maintains compliance with PCI DSS 10.5 and 10.7 requirements to prevent audit logs unauthorized modification or access and retain audit logs history for at least one year.

- **ActionTrail**

  Alibaba Cloud provides the ActionTrail service, which enables a unified log management for cloud resources. The ActionTrail service records user logon and resource access operations under each Alibaba Cloud account. Such record includes the user name (i.e. operator), operation time, source IP address, resource object, operation name, and operation status. With all operation records saved by ActionTrail, customers can perform security analysis, intrusion detection, resource tracking, and compliance audit. If ActionTrail is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the ActionTrail service in a manner that maintains compliance with PCI DSS 10.7 requirement to prevent audit logs unauthorized modification or access and retain audit logs history for at least one year.

- **WAF**

  Based on the big data analyzing capabilities of the cloud security, WAF filters out massive numbers of malicious accesses by defending against SQL injection, XSS, common web server plug-in vulnerabilities, trojan uploads, unauthorized access to resources, and other common OWASP attacks to prevent the leakage of website assets and data and safeguard website security and availability. If WAF is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the WAF service in a manner that maintains compliance with PCI DSS 6.6 requirement.

- **Security Center**

  Alibaba Cloud users can install a Security Center agent on their virtual machine instance, which can work together with the Security Center

for intrusion detection. The intrusion detection for the virtual machine includes remote logon alarm, identification of brute force attack behaviors, webshell detection and removal, and virtual machine anomaly detection. If Security Center is used as PCI DSS compliance solution by customers, it is the customers' responsibility for utilizing the Security Center service in a manner that maintains compliance with PCI DSS 11.4 requirement.

Security Center also provides vulnerability management features for the users. The vulnerability management for the virtual machine incorporates multiple scanning engines (network and local scanning, and vulnerability verification) to thoroughly detect all vulnerabilities in the system at a given time. Features like remote logon alert and one-click webshell removal are provided for a complete vulnerability management experience.

6 References

- Payment Card Industry (PCI) Data Security Standard, version 3.2.1 (May 2018)
  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
- PCI SSC Cloud Computing Guidelines, version 3.0 (April 2018)
  https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf
- Glossary of Terms, Abbreviations, and Acronyms, version 3.2 (April 2016)
  https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf
- Alibaba Cloud Security Whitepaper, version 2.0 (2020)
  https://resource.alibabacloud.com/whitepaper/alibaba-cloud-security-whitepaper---international-edition-v20-2020_1717