Migrating PCI Workloads to VMware Cloud on AWS

vmware®

As organizations extend data centers and migrate applications to the cloud they are looking for a secure platform capable of handling everything from development and test to high volume ecommerce and payment processing. When modernizing and migrating enterprise data centers, architects must carefully consider the implications of leaving the "sensitive" applications behind while the rest make the journey to the cloud. Applications subject to Payment Card Industry (PCI) compliance, including those that process, transmit, or store cardholder data must move to the cloud at the same velocity as the rest of the data center while at the same time adhering to the requirements of the PCI Data Security Standard (PCI DSS).

VMware Cloud on AWS

VMware Cloud™ on AWS brings VMware's enterprise class Software-Defined Data Center software to the AWS Cloud, and enables customers to run production applications across VMware vSphere®-based environments, with optimized access to AWS services. Jointly engineered by VMware and AWS, this on-demand service enables IT teams to seamlessly extend, migrate and manage their cloud-based resources with familiar VMware tools – without the hassles of learning new skills or utilizing new tools. VMware Cloud on AWS integrates VMware's flagship compute, storage and network virtualization products (VMware vSphere, VMware vSAN™ and VMware NSX®) along with VMware vCenter® management as well as robust disaster protection, and optimizes it to run on dedicated, elastic, Amazon EC2 bare-metal infrastructure that is fully integrated as part of the AWS Cloud. This service is delivered and supported by VMware and its partner community. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

VMware Cloud on AWS enables enterprise IT and operations teams to innovate, transform, and add value to the business while continuing to leverage their VMware expertise and without the need to purchase new hardware. With VMware Cloud on AWS you can quickly and confidently migrate applications currently deployed in on-premises and co-located data centers usually without refactoring. In addition, applications deployed in VMware Cloud on AWS become much easier to modernize with high-speed low-latency access to native cloud services from AWS.

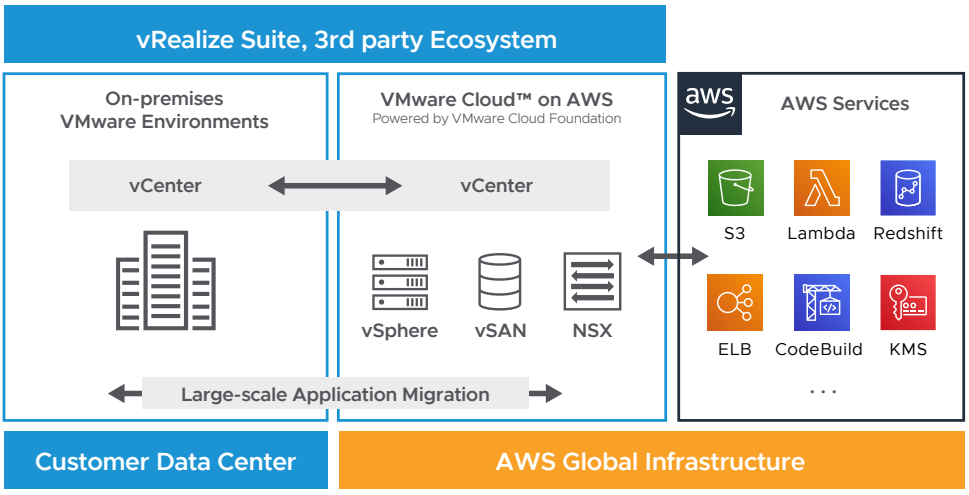

FIGURE 1: VMware Cloud on AWS solution architecture and ecosystem.

VMware Cloud on AWS for PCI DSS workloads

VMware Cloud on AWS provides a consistent operating environment making it easy for customers to adopt the public cloud and accelerates the migration of enterprise applications including PCI DSS and commerce.

Key benefits:

- Shared responsibility model will help enable deployment and operation of PCI DSS workloads
- Consistent environment across vSphere-based private clouds and VMware Cloud on AWS accelerates cloud migrations from months and years to weeks and days by eliminating the rework tax needed to re-architect and re-platform enterprise applications
- Uses familiar skills, tools, and processes for managing cloud environments with consistent operations for improved productivity and reduced costs
- Leverages established on-premises enterprise security, governance, and operational policies, and extends that with the cloud scale and security
- Helps minimize ongoing audit costs by reducing PCI DSS scope and consolidating sensitive applications into isolated SDDCs deployed in VMware Cloud on AWS

Shared responsibility model for VMware Cloud on AWS

VMware Cloud on AWS SDDCs will help provide a compliant environment for PCI DSS workloads underpinned by a shared accountability model where security and compliance responsibilities are shared between AWS, VMware, and the customer. This document provides supplemental guidance covering the responsibilities and ownership of PCI DSS functions when leveraging VMware Cloud on AWS.

Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines and data that reside therein. In addition to determining the configuration work you need to perform as part of your security responsibilities, customers are responsible for managing data (including in-guest encryption options), classifying assets, and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" – VMware is responsible for helping to protect the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

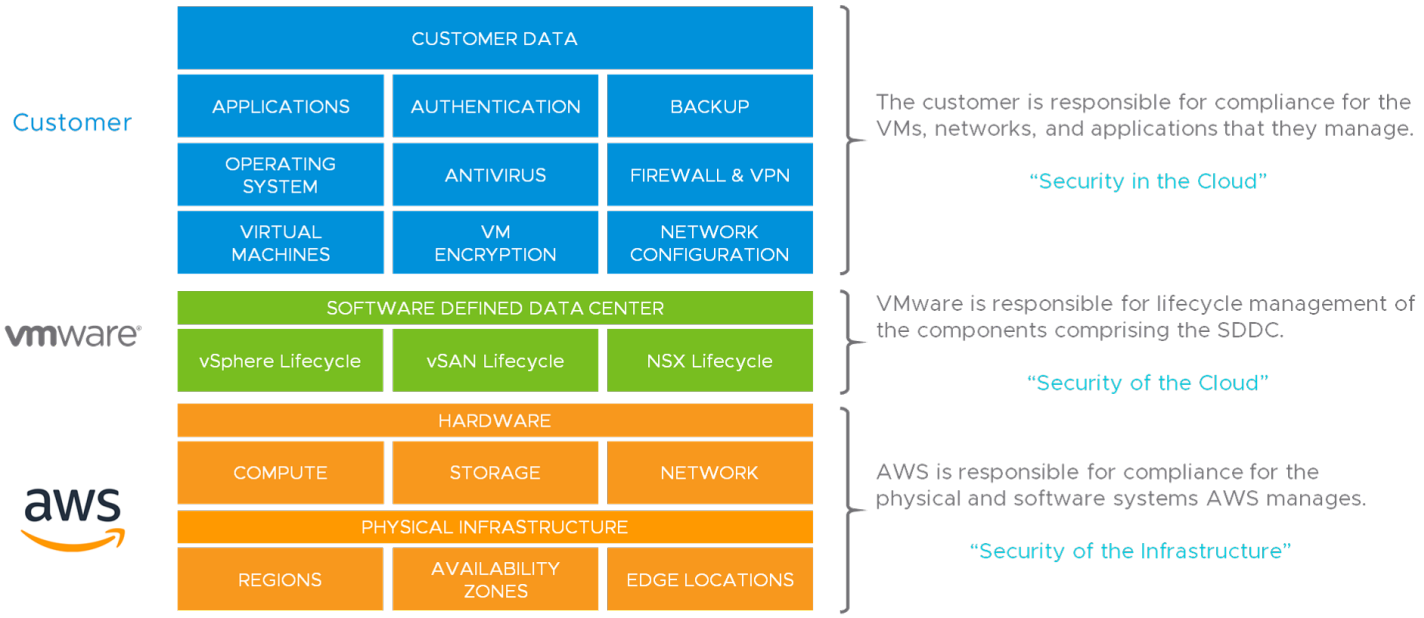

FIGURE 2: VMware Cloud Services architecture and Shared Responsibility Model.

AWS responsibility "Security of the Infrastructure" – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.

Details on the shared responsibility model employed by VMware Cloud on AWS can be found in the table below. You can see that a great deal of low-level operational work is handled by the VMware Cloud on AWS Site Reliability Engineering team leaving the customer to focus on managing their workloads.

RESOURCE	DEPLOYMENT	LIFECYCLE	CONFIGURATION
SERVICE CONSOLE			
console.cloud.vmware.com	VMware	VMware	Customer
vmc.vmware.com	VMware	VMware	Customer
SDDC INFRASTRUCTURE			
Provider VPC	VMware	VMware	VMware
Customer VPC	Customer	Customer	Customer
Bare Metal Hosts	VMware	VMware	VMware
VMware ESXi	VMware	VMware	VMware
VMware vCenter Server	VMware	VMware	VMware
VMware vSAN	VMware	VMware	VMware
VMware NSX-T Manager	VMware	VMware	VMware
SDDC INFRASTRUCTURE			
Management Gateway	VMware	VMware	Customer
Compute Gateway	VMware	VMware	Customer
Virtual Machines	Customer	Customer	Customer
Network Segments	Customer	Customer	Customer
VMware Cloud on AWS Add-On services	Customer	VMware	Customer
ISOs and OVAs	Customer	Customer	Customer
Guest Operating Systems	Customer	Customer	Customer
Logs (vCenter, ESXi, NSX)	Customer	Customer	Customer

Leveraging compliance controls

The Customer and VMware shared responsibility model also extends to IT security and compliance controls. In the same way that VMware and the Customer share operational responsibilities, verification of IT security and compliance controls is also shared. The result of this is that VMware Cloud on AWS helps relieve much of the burden of operating IT security and controls by offloading those associated with the physical infrastructure deployed in the environment. Customers can leverage the published VMware Cloud on AWS controls and documentation to expedite control evaluation and verification procedures as required by their organizations and auditors. VMware Cloud on AWS customers are ultimately responsible for achieving and maintaining their own PCI DSS compliance. The provided shared responsibility model and appendix will be useful references to aid customers in preparing for successful PCI DSS audits by a Qualified Security Assessor (QSA).

Direction

VMware Cloud on AWS has developed new processes and systems that enabled us to become a PCI DSS 3.2.1 Level 1 Service Provider, the highest level of assessment available. This work includes enhancements in security controls and operational processes to meet current and future compliance requirements. This work extends our existing security and compliance footprint that includes SOC 2, ISO 27001, ISO 27017, and ISO 27018.

Conclusion

VMware Cloud on AWS helps enable organizations to meet PCI DSS compliance obligations with an enterprise ready SDDC that provides easy migration, simplifies the movement of workloads, and is supported by a shared responsibility model to maximize flexibility and control. We continuously monitor existing and emerging security standards and integrate applicable requirements into VMware Cloud on AWS. You can view existing compliance and certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance*.

Appendix: Mapping of PCI DSS Controls for VMware Cloud on AWS

The table below details how VMware Cloud on AWS and the Customer leverage the shared responsibility model in order to help meet the requirements of PCI DSS 3.2.1 implementations. The table below describes functionality contained within VMware Cloud on AWS that can help Customers comply with PCI DSS however such functionality alone does not guarantee PCI DSS compliance.

ITEM	DESCRIPTION	VMWARE CLOUD ON AWS CONTROLS	SHARED RESPONSIBILITY
REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA		VMWARE CLOUD ON AWS	CUSTOMER
1.1	Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and stipulate a review of configuration rule sets at least every six months.	The default network configuration provided to each Customer is set to deny all connections into the SDDC. All ports and protocols are disabled except those required by the service. VMware Cloud on AWS has implemented configuration standards for platform firewall and network devices with security testing, change-management and change-control processes in compliance with PCI DSS section 1.	Each VMware Cloud on AWS Customer is responsible for implementing the processes and procedures necessary to ensure that all network connections configured by them for inbound and outbound traffic on any Customer instances deployed on VMware Cloud on AWS comply with the requirements of section 1 of the PCI DSS.
1.2	Build firewall and router configurations that restrict all traffic, inbound and outbound, from “untrusted” networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.	The default network configuration provided to each Customer is set to deny all connections into the SDDC. All ports and protocols are disabled except those required by the service. VMware Cloud on AWS internal production network and systems comply with the requirements of section 1 of the PCI DSS.	Each VMware Cloud on AWS Customer is responsible for implementing the processes and procedures necessary to ensure that all network connections configured by them for inbound and outbound traffic on any Customer instances deployed on VMware Cloud on AWS comply with the requirements of section 1 of the PCI DSS.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	VMware Cloud on AWS provides additional network and host- based protection mechanisms to isolate Customer traffic from the internet and VMware Cloud on AWS platform management traffic.	Each VMware Cloud on AWS Customer is responsible for implementing the processes and procedures necessary to ensure that all network connections configured by them for inbound and outbound traffic on any Customer instances deployed on VMware Cloud on AWS comply with the requirements of section 1 of the PCI DSS.
1.4	Install personal firewall software or equivalent functionality on any 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 cardholder data environment.	Not Applicable No VMware Cloud on AWS devices can connect to the CDE.	Each VMware Cloud on AWS Customer is responsible for ensuring that devices or systems deployed by them that connect to the CDE from the internet are protected with firewall or similar functionality and comply with section 1 of the PCI DSS.

1.5	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 1.
REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS		VMWARE CLOUD ON AWS	CUSTOMER
2.1	Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.	VMware Cloud on AWS has implementation standards and procedures to security harden systems before provisioning into production in compliance with PCI DSS section 2.	Each VMware Cloud on AWS Customer is responsible for removing defaults during their baseline configuration process for all parts of the CDE to meet and maintain the requirements for PCI DSS compliance section 2.
2.2	Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.	VMware Cloud on AWS maintains industry-standard systems security hardening procedures which include multiple vulnerability scans in the software development process and throughout the lifecycle of platform systems in compliance with PCI DSS section 2.	Each VMware Cloud on AWS Customer is responsible for developing hardening standards for all system components deployed by them on VMware Cloud on AWS to meet the requirements for PCI DSS compliance section 2. (Refer to CIS, ISO, SANS and NIST for Standards)
2.3	Using strong cryptography, encrypt all non-console administrative access.	VMware Cloud on AWS enforces the use of strong cryptography for non-console administrative access to VMware Cloud on AWS platform systems. Access is secured by encryption (HTTPS/TLS 1.2) in compliance with PCI DSS section 2.	Each VMware Cloud on AWS Customer is responsible for ensuring the use of strong cryptography for non-console administrative access to VMware Cloud on AWS to meet the requirements for PCI DSS compliance section 2.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	VMware Cloud on AWS maintains a current list of all system components to accurately and securely manage the platform supporting the CDE environment.	Each VMware Cloud on AWS Customer is responsible for managing the inventory of CDE components to meet the requirements for PCI DSS compliance section 2.
2.5	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for ensuring security policies and operational procedures are documented, in use, and known to all affected parties to meet and maintain the requirements for PCI DSS compliance section 2.

2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A1: "Additional PCI DSS Requirements for Shared Hosting Providers."	Not Applicable. VMware Cloud on AWS is not a shared hosting provider. All Customer applications and Customer data are isolated within the SDDC on VMware Cloud on AWS.	Not Applicable. VMware Cloud on AWS is not a shared hosting provider. All Customer applications and Customer data are isolated within the VMware Cloud on AWS.
REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA		VMWARE CLOUD ON AWS	CUSTOMER
3.1	Limit cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.	Not Applicable. VMware Cloud on AWS is an IaaS cloud platform provider and will not have any access to, or responsibility for the management of Customer data.	Each VMware Cloud on AWS Customer retains control and ownership of their Customer Data and it is the Customer's responsibility to manage cardholder data storage retention policies and timely purging of data in accordance with PCI DSS section 3.
3.2	Do not store sensitive authentication data after authorization (even if it is encrypted). See table below. Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.	Not Applicable. VMware Cloud on AWS is an IaaS cloud platform provider and will not have any access to, or responsibility for the management of Customer data.	Each VMware Cloud on AWS Customer retain control and ownership of their Customer Data and it is the Customer's responsibility to store data securely in accordance with PCI DSS section 3.
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt.	Not Applicable. VMware Cloud on AWS is an IaaS cloud platform provider and will not have any access to, or responsibility for the management of Customer data.	Each VMware Cloud on AWS Customer retain control and ownership of their Customer Data and it is the Customer's responsibility to ensure that all data is transmitted and stored securely in accordance with PCI DSS section 3.
3.4	Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)	Not Applicable. VMware Cloud on AWS is an IaaS cloud platform provider and will not have any access to, or responsibility for the management of Customer data.	Each VMware Cloud on AWS Customer retain control and ownership of their Customer Data and it is the Customer's responsibility to store data securely in accordance with PCI DSS section 3.
3.5	Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.	VMware Cloud on AWS Customer data is secured using vSAN XTS AES-256 cipher data-at-rest encryption. VMware Cloud on AWS vSAN data-at-rest encryption keys are protected in compliance with PCI DSS section 3.	Each VMware Cloud on AWS Customer retains control and ownership of their Customer Data and it is the Customer's responsibility to ensure that all in-guest and application data encryption keys are stored securely in accordance with PCI DSS section 3.

3.6	Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.	VMware Cloud on AWS Customer data is secured using vSAN XTS AES-256 cipher data-at-rest encryption in compliance with PCI DSS section 3. All vSAN data, on AWS I3 metal servers, use self-encrypting drives (AES-256-bit encryption). vSAN encryption keys are protected by the AWS KMS. Customers can manage the keys that encrypt their vSAN data by rotating the keys within vSphere UI and API.	Each VMware Cloud on AWS Customer retains control and ownership of their Customer Data and it is the Customer's responsibility to manage encryption keys for in-guest encryption and application data encryption, where implemented by the Customer in accordance with PCI DSS section 3.
3.7	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 3.
REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS		VMWARE CLOUD ON AWS	CUSTOMER
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). 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.	VMware Cloud on AWS provides Customers with the ability to create IPSEC and SSL VPN tunnels from their environments which support the most common encryption methods including AES-256 to meet requirements of PCI DSS section 4. Customers solely manage all external network connectivity to their SDDC environments.	VMware Cloud on AWS Customers solely manage all connectivity to their SDDC environments and are responsible for implementing appropriate security protocols, in compliance with section 4, to protect transmission of their data.
4.2	Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.	Not Applicable. VMware Cloud on AWS personnel do not have access to Customer data. VMware Customers retain control and ownership of their Customer data and it is the Customer's responsibility to ensure that all PAN data is secure and unreadable.	VMware Cloud on AWS Customers solely manage all connectivity to their SDDC environments and are responsible for implementing appropriate security protocols, in compliance with section 4, to protect transmission of their data.
4.3	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 4.

REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS		VMWARE CLOUD ON AWS	CUSTOMER
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.	VMware Cloud on AWS helps ensure all systems commonly affected by malicious software are appropriately protected. For systems not affected commonly by malicious software, periodic evaluations are conducted.	Each VMware Cloud on AWS Customer is responsible for the security of all virtual machines and other resources that are deployed, configured and/or managed as part of the CDE to meet and maintain the requirements for PCI DSS compliance section 5.
5.2	Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.	VMware Cloud on AWS helps ensure all systems commonly affected by malicious software are appropriately protected. For systems not affected commonly by malicious software, periodic evaluations are conducted.	Each VMware Cloud on AWS Customer is responsible for the security of all virtual machines and other resources that are deployed, configured and/or managed as part of the CDE to meet and maintain the requirements for PCI DSS compliance section 5.
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.	VMware Cloud on AWS helps ensure all systems commonly affected by malicious software are appropriately protected. For systems not affected commonly by malicious software, periodic evaluations are conducted.	Each VMware Cloud on AWS Customer is responsible for the security of all virtual machines and other resources that are deployed, configured and/or managed as part of the CDE to meet and maintain the requirements for PCI DSS compliance section 5.
5.4	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for the security of all virtual machines and other resources that are deployed, configured and/or managed as part of the CDE to meet and maintain the requirements for PCI DSS compliance section 5.
REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATION		VMWARE CLOUD ON AWS	CUSTOMER
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	VMware Cloud on AWS has a vulnerability management team dedicated to regularly scan for vulnerabilities across the cloud service platform. All vulnerabilities are scored based on industry risk ranking and are remediated with priority based on risk and criticality to the service in compliance with PCI DSS section 6.	Each VMware Cloud on AWS Customer is responsible for all virtual machines and resources that they deploy, configure and/or manage by implementing a process for identifying and risk ranking vulnerabilities. Customers must meet and maintain the requirements for PCI DSS compliance section 6.

6.2	Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	VMware Cloud on AWS has a vulnerability management team dedicated to regularly scan for vulnerabilities across the cloud service platform. All vulnerabilities are scored based on industry risk ranking and are remediated with priority based on risk and criticality to the service in compliance with PCI DSS section 6.	Each VMware Cloud on AWS Customer is responsible for all protecting all virtual machines and resources that they deploy, configure and/or manage from vulnerabilities by installing applicable vendor supplied patches within one month of release. Customers must meet and maintain the requirements for PCI DSS compliance section 6.
6.3	Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party.	VMware Cloud on AWS applications are developed in accordance with the VMware Security Development Lifecycle (SDL) methodology and meets PCI DSS section 6 requirements.	Each VMware Cloud on AWS Customer is responsible for developing secure software and integrating security into the virtual machines and software applications deployed into the SDDC. Customers must meet and maintain the requirements for PCI DSS compliance section 6.
6.4	Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.	VMware the VMware Cloud on AWS Product Security and product development groups apply an end-to-end set of security testing and change control processes and procedures throughout the software development process, to remediate security issues early in the lifecycle.	Each VMware Cloud on AWS Customer is responsible for change control processes and procedures for all changes to system components and verification after significant change occurs. Customers must meet and maintain the requirements for PCI DSS compliance section 6.
6.5	Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.	The development of the VMware Cloud on AWS Security Development Lifecycle (SDLC) has been heavily influenced by industry best practices and organizations such as SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model). In compliance with PCI DSS compliance section 6, VMware the VMware Cloud on AWS Product Security and product development groups apply an end-to-end set of security testing and change control processes and procedures throughout the software development process, to remediate security issues early in the lifecycle.	Each VMware Cloud on AWS Customer is responsible for implementing secure coding techniques and security testing all applications to protect from vulnerabilities and application exploits. Customers must meet and maintain the requirements for PCI DSS compliance section 6.

6.6	Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by 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.	VMware Cloud on AWS console, (a public-facing web application), is protected by a web-application firewall (WAF) to continuously inspect all network traffic and defend applications by detecting and preventing web-based attacks. As part of the standard VMware SDLC, web application security testing must be completed before any changes are deployed into production. To maintain ongoing VMware Cloud on AWS compliance programs, penetration testing and vulnerability scanning is reviewed in independent 3rd party audits at least annually.	Each VMware Cloud on AWS Customer is responsible for the secure coding of web applications. PCI DSS requires security assessments annually and after significant changes have been made. Customers must meet and maintain the requirements for PCI DSS compliance section 6.
6.7	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 6.
REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED-TO-KNOW		VMWARE CLOUD ON AWS	CUSTOMER
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	VMware Cloud on AWS privileged access is limited by directory services to a team of Support Engineers. Group membership and additional controls are based on the individual's "need to know" to meet job function requirements. All other individuals are denied access. All non-console access is centralized using delegated support access systems and is determined by least privilege with time limited keys to access platform systems supporting the CDE environment. VMware Cloud on AWS personnel do not have access to Customer data.	Each VMware Cloud on AWS Customer is responsible for limiting roles and controlling access to management consoles. Customers must meet and maintain the requirements for PCI DSS compliance section 7.

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.	VMware Cloud on AWS privileged access security policies limit by directory services group membership and additional controls are based on the individual's "need to know" to meet job function requirements. All other individuals are denied access. All non-console access is centralized using delegated support access systems and is determined by least privilege with time limited keys to access platform systems supporting the CDE environment. VMware Cloud on AWS personnel do not have access to Customer data.	Each VMware Cloud on AWS Customer is responsible for security policies and procedures restricting individual access to the cardholder data with least privilege, separation of duties, approval processes, and access reviews. Customers must meet and maintain the requirements for PCI DSS compliance section 7.
7.3	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all policies and procedures related to resources that they deploy, configure and/or manage to restrict access to cardholder data. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 7.
REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS		VMWARE CLOUD ON AWS	CUSTOMER
8.1	Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components. Assign all users a unique username before allowing them to access system components or cardholder data.	All VMware Cloud on AWS employees must use unique accounts for access to platform systems in compliance with PCI DSS section 8. Access is governed by security policies restricting individual access to platform systems supporting the CDE with least privilege, separation of duties, approval processes, user access reviews, and delegated access systems that issue temporary privileged access tokens.	Each VMware Cloud on AWS Customer is responsible for security policies restricting individual access to the CDE with least privilege, separation of duties, approval processes, and user access reviews. Customers must meet and maintain the requirements for PCI DSS compliance section 8.
8.2	Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.	VMware Cloud on AWS uses MFA as an additional safeguard to the delegated access system that provides temporary privileged access to platform systems supporting the CDE. Strong authentication, communications and passwords are secured by using strong cryptography.	Each VMware Cloud on AWS Customer is responsible for enforcing PCI DSS compliant password policy and deploying MFA for all users that access the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 8.

8.3	Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity's network.	VMware Cloud on AWS uses MFA as an additional safeguard to the delegated access system that provides temporary privileged access to platform systems and the CDE.	Each VMware Cloud on AWS Customer is responsible for implementing multi-factor authentication mechanisms for access to the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 8.
8.4	Develop, implement, and communicate authentication policies and procedures to all users.	VMware Cloud on AWS security policies and operational procedures are well documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all authentication policies and procedures. Customers must meet and maintain the requirements for PCI DSS compliance section 8.
8.5	Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to Customer environments must use a unique authentication credential (such as a password/passphrase) for each Customer environment.	VMware Cloud on AWS personnel have unique authentication credentials for accessing the CDE.	Each VMware Cloud on AWS Customer is responsible for all authentication credentials used to access systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 8.
8.6	Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.	VMware Cloud on AWS employees are assigned individual security tokens and certificates for authentication.	Each VMware Cloud on AWS Customer is responsible for all authentication mechanisms that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 8.
8.7	All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).	Not Applicable: VMware Cloud on AWS does not require any account creation or access to Customer databases In compliance with PCI DSS section 8, VMware Cloud on AWS Customers retain control and ownership of their Customer data and it is the Customer's responsibility to restrict all access to the CDE.	Each VMware Cloud on AWS Customer is responsible for all database access security that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 8.

8.8	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 8.
REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA		VMWARE CLOUD ON AWS	CUSTOMER
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Not Applicable Physical datacenters are AWS managed and controlled. AWS is a Payment Card Industry Data Security Standard (PCI DSS) compliant service provider (since 2010). Note: Customers are responsible for collecting PCI DSS Attestation of Compliance (AOC) and Responsibility Summary documents from AWS.	Not Applicable
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.	Not Applicable Physical datacenters are AWS managed and controlled.	Not Applicable
9.3	Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked promptly upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled.	Not Applicable Physical datacenters are AWS managed and controlled.	Not Applicable
9.4	Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.	Not Applicable Physical datacenters are AWS managed and controlled.	Not Applicable

9.5	Physically secure all media; store media back-ups in a secure location, preferably off site.	Not Applicable VMware Cloud on AWS does not provide Customer data backup/ archive services.	Each VMware Cloud on AWS Customer is responsible for maintaining control of all data stored outside of the VMware Cloud on AWS SDDC environment. Customers must meet and maintain the requirements for PCI DSS compliance section 9.
9.6	Maintain strict control over the internal or external distribution of any kind of media.	Not Applicable VMware Cloud on AWS does not provide Customer data backup/ archive services.	Each VMware Cloud on AWS Customer is responsible for all backup systems and distribution related to media. Customers must meet and maintain the requirements for PCI DSS compliance section 9.
9.7	Maintain strict control over the storage and accessibility of media.	Not Applicable VMware Cloud on AWS does not provide Customer data backup/ archive services.	Each VMware Cloud on AWS Customer is responsible for all media inventory management, access, and storage policy. Customers must meet and maintain the requirements for PCI DSS compliance section 9.
9.8	Destroy media when it is no longer needed for business or legal reasons.	Not Applicable VMware Cloud on AWS does not provide Customer data backup/ archive services.	Each VMware Cloud on AWS Customer is responsible for securely destroying electronic media. Customers must meet and maintain the requirements for PCI DSS compliance section 9.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.	Not Applicable	Each VMware Cloud on AWS Customer is responsible for protecting cardholder data related devices. Customers must meet and maintain the requirements for PCI DSS compliance section 9.
9.10	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	Not Applicable Physical datacenters are AWS managed and controlled.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 9.

REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA		VMWARE CLOUD ON AWS	CUSTOMER
10.1	Implement audit trails to link all access to system components to each individual user.	VMware Cloud on AWS implements audit trails to link all VMware Cloud on AWS user access to platform system components and to the CDE by each individual user.	Each VMware Cloud on AWS Customer is responsible for recording and maintaining audit trails for all access by individual users to the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.2	Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.	VMware Cloud on AWS restricts access to only authorized personnel to meet needs of job functions with least privilege principles. All root or administrative activity supporting the cloud platform and CDE is automatically recorded in audit trails.	Each VMware Cloud on AWS Customer is responsible for audit trails for all system components of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.3	Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.	VMware Cloud on AWS audit trail entries are automatically recorded for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.	Each VMware Cloud on AWS Customer is responsible for audit trails for all system components of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.4	Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.	VMware Cloud on AWS has established procedures ensuring centralized time server technologies are used to synchronize VMware Cloud on AWS platform systems and services.	Each VMware Cloud on AWS Customer is responsible for time-synchronization on all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.5	Secure audit trails so they cannot be altered.	VMware Cloud on AWS platform systems and services audit trails are automatically secured and monitored in accordance with a standard policy that prevents any alteration.	Each VMware Cloud on AWS Customer is responsible for securing audit trails for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.

10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.	VMware Cloud on AWS operational environment supports real-time analysis of audit trails and security events to identify anomalies or suspicious activity that could indicate a potential compromise.	Each VMware Cloud on AWS Customer is responsible for reviewing audit trails and security events for system components they manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.7	Retain audit trail history for at least one year; at least three months of history must be promptly available for analysis.	VMware Cloud on AWS has implemented an audit trail standard with a at least one-year retention policy and at least three months of history promptly available for analysis.	Each VMware Cloud on AWS Customer is responsible for retaining audit trails for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.8	Service providers must implement a process for timely detection and reporting of failures of critical security control systems.	The VMware Security Operations Center has a process for timely detection and reporting of failures of critical security control systems.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 10.
10.9	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 10.
REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES		VMWARE CLOUD ON AWS	CUSTOMER
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. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.	Not Applicable No wireless devices can connect to the VMware Cloud on AWS platform networks.	Not Applicable

11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.	VMware Cloud on AWS vulnerability management team conducts internal and external vulnerability scans at least quarterly and after significant network changes. External in-scope systems are scanned using an Approved Scanning Vendor (ASV).	Each VMware Cloud on AWS Customer is responsible for performing quarterly internal and external vulnerability scans, rescans using an Approved Scanning Vendor (ASV) as needed against all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 11.
11.3	Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls.	VMware Cloud on AWS performs penetration testing on the entire CDE perimeter and critical systems. Penetration testing is conducted at least annually and after any significant network change to meet requirements for current compliance programs.	Each VMware Cloud on AWS Customer is responsible for implementing a penetration testing methodology that meets PCI DSS requirements for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 11.
11.4	Use network 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 inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.	VMware Cloud on AWS network intrusion detection and intrusion prevention techniques detect and prevent intrusions into the network.	Each VMware Cloud on AWS Customer is must deploy, configure and manage techniques to detect and/or prevent intrusions into CDE networks. Customers must meet and maintain the requirements for PCI DSS compliance section 11.
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 data files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.	VMware Cloud on AWS cloud platform change detection mechanisms alert VMware personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or data files.	Each VMware Cloud on AWS Customer is must deploy, configure and manage change detection mechanisms to alert personnel to unauthorized modification of critical system files, configuration files or data files. Customers must meet and maintain the requirements for PCI DSS compliance section 11.

11.6	Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 11.
REQUIREMENT 12: MAINTAIN AN INFORMATION SECURITY POLICY		VMWARE CLOUD ON AWS	CUSTOMER
12.1	Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.	VMware Cloud on AWS security policy is published, maintained and mandatory training is provided to all employees annually.	Each VMware Cloud on AWS Customer is responsible all activities related to their annual security policy programs. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.2	Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.	VMware Cloud on AWS has a formal annual risk assessment process that is performed.	Each VMware Cloud on AWS Customer is responsible all activities related to their annual risk assessment process. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.3	Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.	VMware Cloud on AWS has a formal acceptable use policy, information security policies and standards for all personnel.	Each VMware Cloud on AWS Customer is responsible all activities related to their annual usage policy programs. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.	VMware Cloud on maintains PCI DSS related security policies and procedures to clearly define information security responsibilities for all personnel.	Each VMware Cloud on AWS Customer is responsible for policies for acceptable use, authentication, and implementation for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.5	Assign to an individual or team information security responsibilities defined by 12.5 subsections.	VMware Cloud on AWS maintains personnel assignments for information security responsibilities.	Each VMware Cloud on AWS Customer is responsible for defining and assigning information security responsibilities to their employees. Customers must meet and maintain the requirements for PCI DSS compliance section 12.

12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	VMware Cloud on AWS maintains a formal security awareness program that addresses cardholder data security policies and procedures.	Each VMware Cloud on AWS Customer is responsible for security awareness policies that govern how their employees access the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.	VMware employment policy includes screening of candidates employment history, criminal record, credit history and reference checks.	Each VMware Cloud on AWS Customer is responsible for ensuring employees with access to the CDE have all passed background checks. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.8	Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.	VMware Cloud on AWS and supporting service providers do not have access to cardholder data.	Each VMware Cloud on AWS Customer is responsible for monitoring PCI DSS compliance for the service providers that can affect the security of the CDE or where cardholder data is shared. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.9	Service providers acknowledge in writing to Customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the Customer, or to the extent they could impact the security of the Customer's cardholder data environment.	VMware Cloud on AWS's Customers are informed in writing that VMware Cloud on AWS does not have access to cardholder data.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 12.
12.10	Implement an incident response plan. Be prepared to respond promptly to a system breach.	VMware Cloud on AWS has a formal incident response plan to promptly address a system breach.	Each VMware Cloud on AWS Customer is responsible for implementing an incident response plan for all systems and data that they deploy as part of the CDE. Customers must meet and maintain the requirements for PCI DSS compliance section 12.
12.11	Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.	VMware Cloud on AWS maintains security policies and operational procedures to make sure they are documented, in use, and known to all affected parties.	Each VMware Cloud on AWS Customer is responsible for all systems and resources that they deploy, configure and/or manage as part of the CDE. Customers must meet and maintain the related security policies and operational procedures requirements for PCI DSS compliance section 12.

* Customer data is content/data that customers have uploaded to or created within their SDDC on VMware Cloud on AWS.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com