VMware Solution Guide for

Payment Card Industry (PCI)

September 2012

v1.3

VALIDATION DOCUMENT

vmware®

Table of Contents

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

Introduction

Compliance and security continue to be top concerns for organizations that plan to move their environment to cloud computing. VMware helps organizations address these challenges by providing bundled solutions (suites) that are designed for specific use cases. These use cases address questions like "How to be PCI compliant in a VMware Private Cloud" by providing helpful information for VMware architects, the compliance community, and third parties.

The PCI Private Cloud Use Case is comprised of four VMware Product Suites - vCloud, vCloud Networking and Security, vCenter Operations (vCOPs) and View. These product suites are described in detail in this paper. The use case also provides readers with a mapping of the specific PCI controls to VMware's product suite, partner solutions, and organizations involved in PCI Private Clouds. While every cloud is unique, *VMware and its partners can provide a solution that addresses over 70% of the PCI DSS requirements.*

Figure 1: PCI Requirements

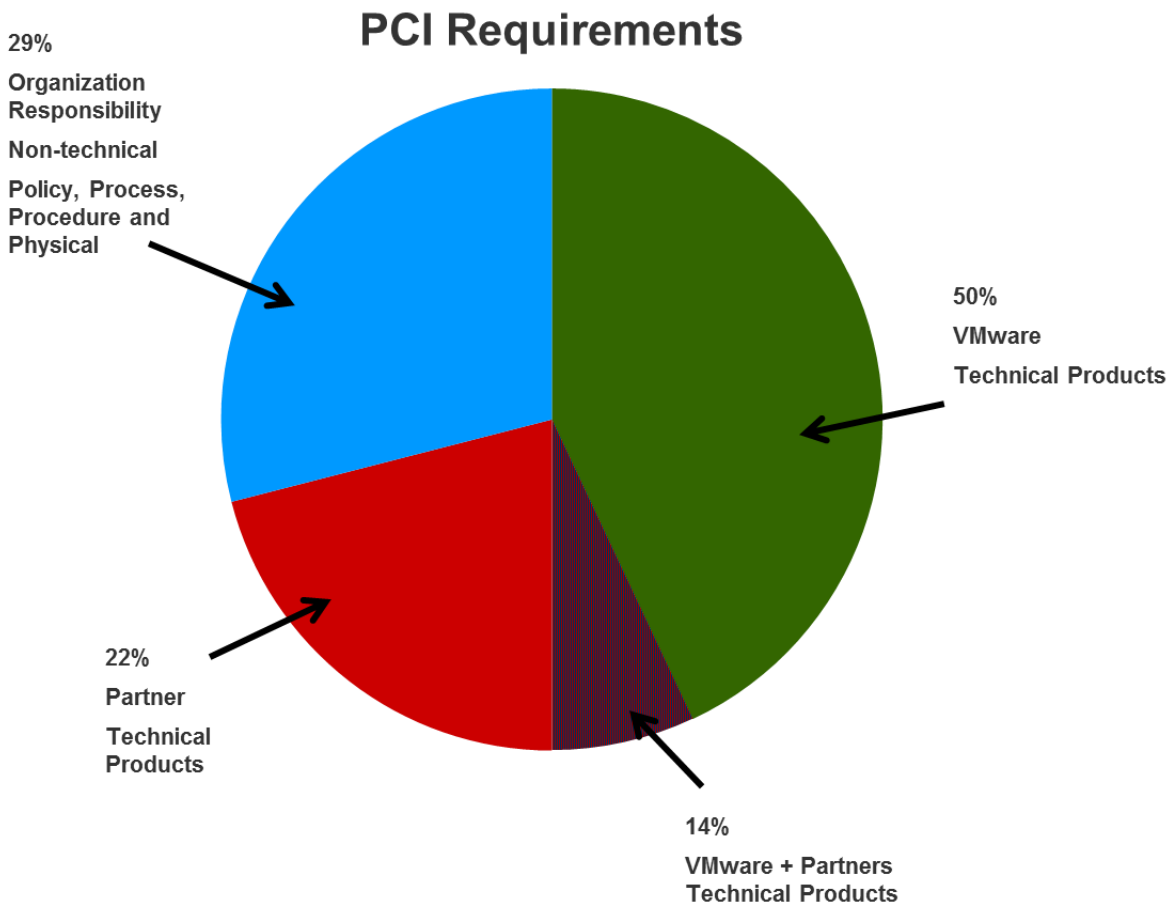
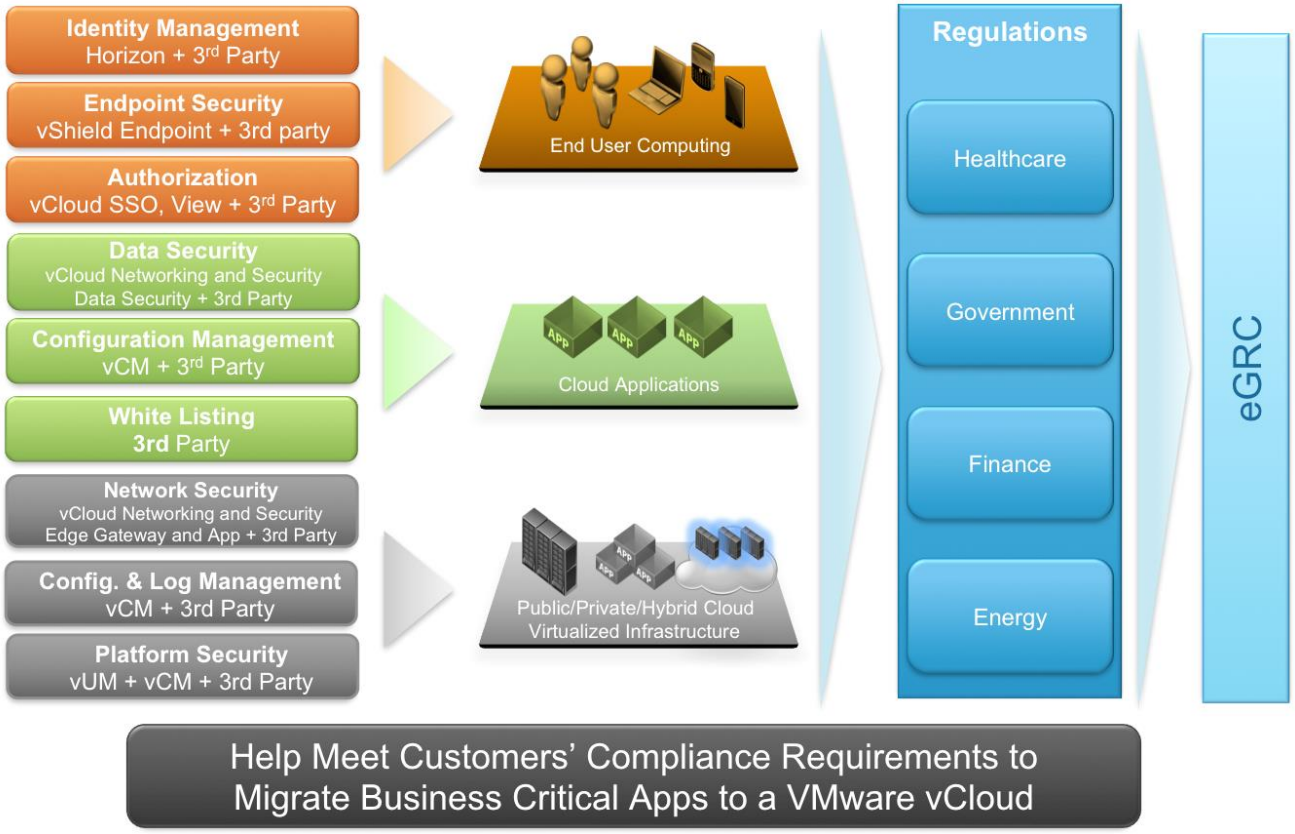


Figure 2: VMware + Partner Product Capabilities for a Trusted Cloud



Overview of PCI as it applies to Cloud/Virtual Environments

The PCI Security Standards Council (SSC) was established in 2006 by five global payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.). The payment brands require through their Operating Regulations that any merchant or service provider must be PCI compliant. Merchants and service providers are required to validate their compliance by assessing their environment against nearly 300 specific test controls outlined in the PCI Data Security Standards (DSS). Failure to meet PCI requirements may lead to fines, penalties, or inability to process credit cards in addition to potential reputational loss.

The PCI DSS has six categories with twelve total requirements as outlined below:

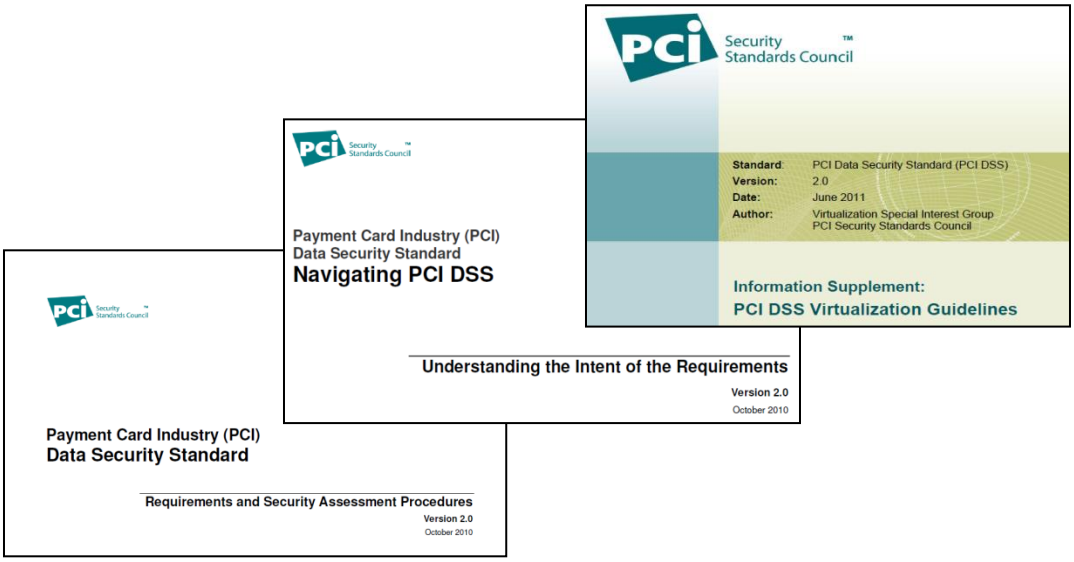
Table 1: PCI Data Security Standard

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

The PCI SSC specifically began providing formalized guidance for cloud and virtual environments in October, 2010. These guidelines were based on industry feedback, rapid adoption of virtualization technology, and the move to cloud. Version 2.0 of the Data Security Standard (DSS) specifically mentions the term “virtualization” (previous versions did not use the word “virtualization”). This was followed by an additional document explaining the intent behind the PCI DSS v2.0, “Navigating PCI DSS”. These documents were intended to clarify that virtual components should be considered as “components” for PCI, but did not go into the specific details and risks relating to virtual environments. Instead, they address virtual and cloud specific guidance in an Information Supplement, “PCI DSS Virtualization Guidelines,” released in June 2011 by the PCI SSC’s Virtualization Special Interest Group (SIG).

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

Figure 3: Navigating PCI DSS



The virtualization supplement was written to address a broad set of users (from small retailers to large cloud providers) and remains product agnostic (no specific mentions of vendors and their solutions).

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of competent legal counsel.

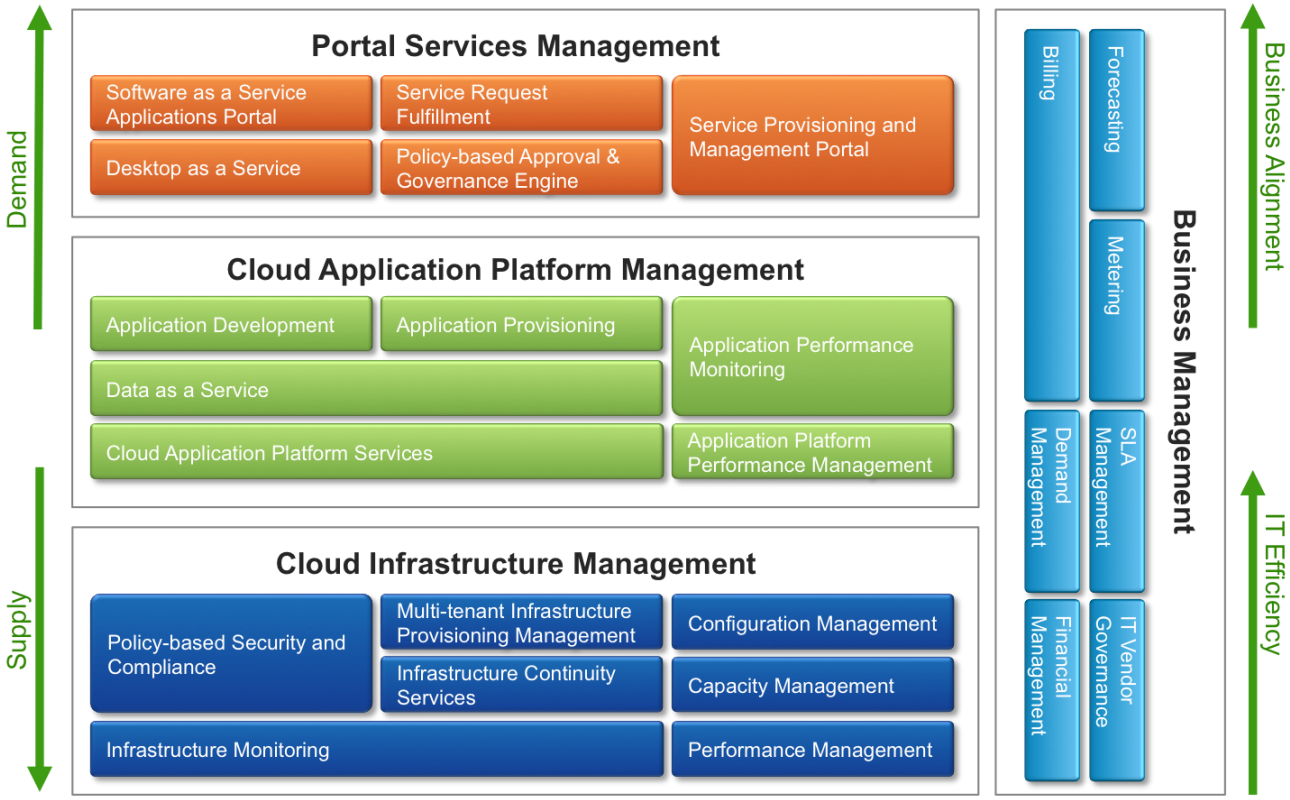
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Cloud Computing

Cloud computing and virtualization have continued to grow significantly every year. There is a rush to move applications and even whole datacenters to the "cloud", although few people can succinctly define the term "cloud computing." There are a variety of different frameworks available to define the cloud, and their definitions are important as they serve as the basis for making business, security, and audit determinations. VMware defines cloud or utility computing as the following (http://www.vmware.com/solutions/cloud-computing/public-cloud/faqs.html):

"Cloud computing is an approach to computing that leverages the efficient pooling of on-demand, self-managed virtual infrastructure, consumed as a service. Sometimes known as utility computing, clouds provide a set of typically virtualized computers which can provide users with the ability to start and stop servers or use compute cycles only when needed, often paying only upon usage.."

Figure 4: Cloud Computing



There are commonly accepted definitions for the cloud computing deployment models and there are several generally accepted service models. These definitions are listed below:

- Private Cloud – The cloud infrastructure is operated solely for an organization and may be managed by the organization or a third party. The cloud infrastructure may be on-premise or off-premise.
- Public Cloud – The cloud infrastructure is made available to the general public or to a large industry group and is owned by an organization that sells cloud services.

- Hybrid Cloud – The cloud infrastructure is a composition of two or more clouds (private and public) that remain unique entities, but are bound together by standardized technology. This enables data and application portability; for example, cloud bursting for load balancing between clouds. With a hybrid cloud, an organization gets the best of both worlds, gaining the ability to burst into the public cloud when needed while maintaining critical assets on-premise.
- Community Cloud – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on-premise or off premise.

To learn more about VMware's approach to cloud computing, review the following:

- http://www.vmware.com/solutions/cloud-computing/index.html#tab3 - VMware Cloud Computing Overview
- http://www.vmware.com/cloud-computing/cloud-architecture/vcat-toolkit.html - VMware's vCloud Architecture Toolkit

When an organization is considering the potential impact of cloud computing to their highly regulated and critical applications, they may want to start by asking:

- Is the architecture a true cloud environment (does it meet the definition of cloud)?
- What service model is used for the cardholder data environment (SaaS, PaaS, IaaS)?
- What deployment model will be adopted?
- Is the cloud platform a trusted platform?

The last point is critical when considering moving highly regulated applications to a cloud platform. PCI does not endorse or prohibit any specific service and deployment model. The appropriate choice of service and deployment models should be driven by customer requirements, and the customer's choice should include a cloud solution that is implemented using a trusted platform.

VMware is the market leader in virtualization, the key enabling technology for cloud computing. VMware's vCloud Suite is the trusted cloud platform that customers use to realize the many benefits of cloud computing including safely deploying business critical applications.

To get started, VMware recommends that all new customers undertake a compliance assessment of their current environment. VMware offers free compliance checkers that are based on VMware's vCenter Configuration Manager solution. Customers can simply point the checker at a target environment and execute a compliance assessment request. The resultant compliance report provides a detailed 'rule by rule' indication of pass or failure against a given standard. Where compliance problems are identified, customers are directed to a detailed knowledge base for an explanation of the rule violated and information about potential remediation. To download the free compliance checkers click on the following link:

https://my.vmware.com/web/vmware/evalcenter?p=compliance-chk&lp=default&cid=70180000000MJsMAAW

If you are an organization or partner that is interested in more information on the VMware Compliance Program, please email us at compliance-solutions@vmware.com

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

Where to Start - Considerations for Management, IT and Auditors

Migrating a traditional IT infrastructure to a virtual or cloud environment has a significant impact on an organization that extends beyond information technology. Security and compliance continue to remain top concerns for management, IT departments, and auditors. All three areas should be represented and engaged for any IT virtualization or cloud projects to confirm that business, IT operations, and compliance teams carefully consider the benefits and risks. The move to cloud and virtual environments has many technical considerations, but it should also be a business decision. Organizations should review the benefits and risks of their current environment and compare them to the different cloud deployment models and service models.
The following questions may be important when considering the potential business impact, benefits, and risks of a virtual and/or cloud environment.

Management/Business Considerations

1. Can the Cloud be a strategic differentiator for the business or is it a commodity service?
2. How are competitors or partners leveraging Cloud and virtualization?
3. What is the business value that Cloud could deliver to Operations?
4. What is the strategic value that Cloud could deliver to the Company?
5. Is the IT Budget expanding or contracting?
6. What are the areas where Cloud can provide additional value to the company?
7. Are there efforts to consolidate IT functions that can be addressed with Cloud?
8. What are the critical IT services that are or could be outsourced?

IT Considerations

1. How does the IT Operations plan address the company's strategic and operational goals?
2. What manual processes are in place that can be automated?
3. What are the skills and capabilities of the IT Department?
4. Have there been any previous attempts to virtualize or outsource critical operations?
5. Which IT initiatives currently underway could affect the scope of the Cardholder Data Environment?
6. How is encryption and tokenization currently used to limit risk?
7. How is sensitive data currently classified (i.e., do you know where all your PCI data resides)?
8. Are there secondary systems that might have credit card data (accounting, marketing)?
9. How has security and compliance affected IT Operations?

Audit Considerations

1. What prior experience does the auditor have with virtual environments (Qualified Security Assessor (QSA) or Internal Security Assessor (ISA))?
2. Has the QSA or ISA successfully assessed PCI environments in the cloud or virtual areas?
3. What certifications do they have in VMware products or solutions?
4. How many individuals that are part of the assessment team have experience with VMware?
5. What thought leadership and guidance has the QSA/ISA published?
6. What are the risks and mitigation techniques the QSA/ISA believes are appropriate for multi-tenancy or mixed-mode environments?
7. How long have they been working with VMware architectures?
8. Have they been involved with the PCI Special Interest Group or other PCI communities?
9. What references do they have for conducting similar assessments?
10. Is the QSA/ISA assigned to the audit engagement company knowledgeable about the basic components, systems, and software in a VMware cloud?

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

Guidance from the Payment Card Industry Security Standards Council

The PCI SSC has issued several documents that provide guidance for interpreting the Data Security Standard and implementing compliant virtual and Cloud environments. VMware has extracted several paragraphs from these documents that highlight some of the critical requirements/guidance that organizations are required to address as part of their deployments. VMware has also provided information regarding how VMware tools are designed to help organizations address these controls.

PCI DSS	Payment Card Industry Data Security Standard v2.0 – October 2010
NAV	Navigating PCI DSS
SUP	PCI DSS Virtualization Guidelines

Table 2: PCI Guidance

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
PCI DSS	10	The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. "System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.	In a VMware environment there are many system components, which should be considered as part of the virtual environment beyond the physical components (ESXi hosts, SANs, network devices). These include vCenter Servers, vCenter Databases, VUM, virtual switches, etc. It is important to consider all the virtual components that are installed and support the VMware environment.
PCI DSS	10	Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended…	VMware strongly recommends that organizations implement segmentation in order to separate the cardholder data environment (CDE) from the Non- CDE.
PCI DSS	11	Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.	When properly implemented, VMware's products can support the control requirement for segmentation in multi-tenant, mixed-mode environments.
PCI DSS	11	At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.	VMware recommends that organizations leverage vCloud Networking and Security App and Edge Gateway in order to implement network segmentation in a cloud environment. App can be used to properly segment virtual machines from each other. Edge Gateway can be used to provide an additional layer of protection by isolating the private cloud network from an untrusted outside network.

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

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
PCI DSS	25	Requirement 2.2.1 Implements 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.	PCI DSS 2.0 clarifies that multiple virtual machines of different functions can reside on the same physical hardware.
NAV	4	Qualified Security Assessor (QSA) can assist in determining scope within an entity's cardholder data environment along with providing guidance about how to narrow the scope of a PCI DSS assessment by implementing proper network segmentation.	If an organization plans to use a QSA, VMware recommends they engage the QSA during the design phase. This ensures that the assessor and the organization are aligned to the risks and technologies deployed. VMware recommends that organizations work with assessors that are familiar with the technology and organizations should have dedicated specialists that understand both the PCI requirements and VMware capabilities.
NAV	5	All components within the virtual environment will need to be identified and considered in scope for the review, including the individual virtual hosts or devices, guest machines, applications, management interfaces, central management consoles, hypervisors, etc.	Several features are embedded into VMware's products to identify the hosts, virtual machines, components, databases, and communication paths of the Cloud environment.
NAV	5	The implementation of a virtualized environment must meet the intent of all requirements, such that the virtualized systems can effectively be regarded as separate hardware.	When implementing a VMware environment, organizations should ask what risks other hosts and virtual components present to the CDE. In addition to supporting the proper segmentation of the production systems, organizations should review backup, disaster recovery, and storage systems with a view to properly protecting that cardholder data in the Cloud.
NAV	12	(Guidance for Requirement 1.1.2) - Network and data flow diagrams should include virtual system components and document Intra-host data flows.	vCloud Networking and Security App provides solutions to monitor and control intra-host communication of a cloud environment. Organizations should strive to properly map the Cloud management infrastructure as well as the intra-host communication paths, particularly for virtual machines that are within a common VLAN.
NAV	18	Where virtualization technologies are used, each virtual component (e.g. virtual machine, virtual switch, virtual security appliance, etc.) should be considered a "server" boundary. Individual hypervisors may support different functions, but a single virtual machine should adhere to the "one primary function" rule.	PCI DSS 2.0 clarifies that multiple virtual machines of different functions can reside on the same physical hardware. If different security zones (such as DMZ's and Internal Networks) reside on shared hypervisors, each virtual server should still meet the "one primary function" rule and be logically separated from virtual servers of different functions. For example, vCloud Networking and Security

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

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
			App can be used to create a DMZ segmenting a virtual web server from a virtual database server.
SUP	3	There are four simple principles associated with the use of virtualization in cardholder data environments: a. If virtualization technologies are used in a cardholder data environment, PCI DSS requirements apply to those virtualization technologies. b. Virtualization technology introduces new risks that may not be relevant to other technologies, and that must be assessed when adopting virtualization in cardholder data environments. c. Implementations of virtual technologies can vary greatly, and entities will need to perform a thorough discovery to identify and document the unique characteristics of their particular virtualized implementation, including all interactions with payment transaction processes and payment card data. d. There is no one-size-fits-all method or solution to configure virtualized environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented.	VMware has embraced the guidance from the PCI SSC and is actively publishing product guidance aligned to the core principals and intent of the PCI DSS and applicable information supplements. VMware understands that every cloud and every implementation is unique, and has provided implementation procedures, hardening documents, and compliance frameworks to help organizations properly evaluate the risks and benefits of PCI Clouds. When properly deployed, VMware's solutions confirm that multi-tenant, mixed mode clouds can be compliant with the standards of today and tomorrow.
SUP	7, 8	Scope Guidance: If any virtual component connected to (or hosted on) the hypervisor is in scope for PCI DSS, the hypervisor itself will always be in scope. Virtual Appliances used to connect or provide services to in-scope system components or networks would be considered in-scope. Any VSA/SVA that could impact the security of the CDE would also be considered in scope.	In order to maximize the benefits and features of the vSphere App and Cloud architectures, VMware recommends that the entire vSphere architecture (including ESXi hosts, vSwitches, and vCenter servers and databases) be considered in scope and properly protected for most environments. If host or management components (such as vCenter) are not included, organizations must ensure that they do not have access to virtual components within the CDE and do not have any connectivity into the CDE.
SUP	8	Networks provisioned on a hypervisor-based virtual switch will be in scope if provisioned with an in-scope component or if they provide services or connect to an in-scope component. Physical devices hosting virtual switches or routers would be considered in scope if any of the hosted components connects to an in-scope network.	Organizations should confirm that anytime cardholder data flows through vSwitches or virtual Distributed Switches that such data is properly documented and segmented. This often includes pairing hypervisor based virtual switches with specialized physical core switches and routers, which are designed for the VMware infrastructure. vCloud Networking and Security App can help organizations manage the network segmentation by providing control at the virtual switch level.

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

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
SUP	9	The use of cloud computing presents a number of scoping challenges and considerations. Entities planning to use cloud computing for their PCI DSS environments should first ensure that they thoroughly understand the details of the services being offered, and perform a detailed assessment of the unique risks associated with each service. Additionally, as with any managed service, it is crucial that the hosted entity and provider clearly define and document the responsibilities assigned to each party for maintaining PCI DSS requirements and any other controls that could impact the security of cardholder data.	Every cloud is different based on the technology deployed and the business processes utilized. VMware's cloud provides a robust set of suites and features which helps automate and provide transparency of controls within the Cloud. If an organization is going to act as a provider of cloud services to other merchants or service providers, the Cloud provider should be specific on what services are in PCI scope, how they have been validated to be effective, and what controls are specifically not in scope with respect to their solution.
SUP	9	The cloud provider should clearly identify which PCI DSS requirements, system components, and services are covered by the cloud provider's PCI DSS compliance program. Any aspects of the service not covered by the cloud provider should be identified, and it should be clearly documented in the service agreement that these aspects, system components, and PCI DSS requirements are the responsibility of the hosted entity to manage and assess. The cloud provider should provide sufficient evidence and assurance that all processes and components under their control are PCI DSS compliant.	VMware recommends that organizations establish a "PCI Requirements Matrix" or similar document to clearly communicate the extent of services a Cloud provider offers and include details regarding the scope, controls, and validation, which has been performed to confirm that the Cloud Providers' controls are sufficient.
SUP	10	A key risk factor unique to virtual environments is the hypervisor—if this is compromised or not properly configured, all VMs hosted on that hypervisor are potentially at risk. The hypervisor provides a single point of access into the virtual environment and is also potentially a single point of failure. Misconfigured hypervisors could result in a single point of compromise for the security of all hosted components.	VMware provides extensive product guidance to establish that virtual components and hypervisors are fully patched and configured appropriately. The combination of vCenter, VUM, and VCM help track and enforce the patching and security configuration of critical components in the VMware Cloud.
SUP	12	Inactive VMs containing payment card data can become unknown, unsecured data stores, which are often only rediscovered in the event of a data breach. Because dormant VMs are not actively used, they can easily be overlooked and inadvertently left out of security procedures.	A VM is simply a set of software files, which are executed when run in the context of a hypervisor. Tools such as VCM can be used to monitor and update dormant VM's, providing better than physical patching and signature updates for virtual components when properly implemented.
SUP	13	Specialized tools for monitoring and logging virtual environments may be needed to capture the level of detail required from the multiple components, including hypervisors, management interfaces, virtual machines, host systems, and virtual appliances.	VMware has an extensive set of features for management, monitoring, and logging. In addition, several API's and features have been implemented which allow critical system files, logs, and access control mechanisms to be centrally monitored and correlated with industry leading SIEM solutions.

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

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
SUP	11, 20	The risk of hosting VMs of different trust levels on the same host needs to be carefully assessed. In the virtual context, a VM of lower trust will typically have lesser security controls than VMs of higher trust levels. The lower-trust VM could therefore be easier to compromise, potentially providing a stepping stone to the higher-risk, more sensitive VMs on the same system. It is strongly recommended (and a basic security principle) that VMs of different security levels are not hosted on the same hypervisor or physical host; the primary concern being that a VM with lower security requirements will have lesser security controls, and could be used to launch an attack or provide access to more sensitive VMs on the same system.	The architecture of VMware's hypervisor, ESXi, significantly limits the attack profile compared to competitive hypervisor offerings. The design provides more security control and significantly reduces the risk that non PCI-compliance VM's pose to the cardholder data environment. In addition, segmentation of different trust levels on the same host is readily accomplished using virtual Distributed Switch and vCloud Networking and Security App. vDS, vCloud Networking and Security Edge Gateway and vCloud Networking and Security App enable creation of rules to control traffic flows within the virtual environment.
SUP	20	As a general rule, any VM or other virtual component that is hosted on the same hardware or hypervisor as an in-scope component would also be in scope for PCI DSS, as both the hypervisor and underlying host provide a connection (either physical, logical, or both) between the virtual components, and it may not be possible to achieve an appropriate level of isolation, or segmentation, between in-scope and out-of-scope components located on the same host or hypervisor.	Similar to all technology, as virtualization and cloud computing have evolved so has the ability to provide proper levels of isolation. Segmentation of different trust levels on the same host is readily accomplished using virtual Distributed Switch and vCloud Networking and Security App. In addition vDS, vCloud Networking and Security Edge Gateway and App enable creation of rules to control traffic flows within the virtual environment.
SUP	21	In order for in-scope and out-of-scope VMs to co-exist on the same host or hypervisor, the VMs must be isolated from each other such that they can effectively be regarded as separate hardware on different network segments with no connectivity to each other. Any system components shared by the VMs, including the hypervisor and underlying host system, must therefore not provide an access path between the VMs.	Organizations can use orchestration processes or virtual profiles to confirm that any provisioned hosts and/or virtual components are locked down and do not have any unnecessary connectivity. VCM can be used to identify misconfigurations of running and offline machines. Segmentation of different trust levels on the same host is readily accomplished using virtual Distributed Switch (vDS) and vCloud Networking and Security App. In addition vDS, vCloud Networking and Security Edge Gateway and App enable creation of rules to control traffic flows within the virtual environment.
SUP	21	All existing out-of-band channels should be identified and documented—whether they are actively used or not—and appropriate controls implemented to isolate workloads and virtual components.	In the ESXi architecture, many out of band channels have been eliminated to reduce the complexity and risk to the hypervisor. VMware has also provided features that enable management processes to flow through centralized points

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

SOURCE	PAGE	PCI GUIDANCE	VMWARE SOLUTIONS
			(such as vCenter) that can be used to control access, logging, and monitoring functions. Organizations can also limit the impact of out-of-band channels by implementing policies to reduce the risk (such as prohibiting dirty snapshots and enabling snapshots to only be maintained for a brief period of time).

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

PCI Compliance Stack

VMware provides an extensive suite of products designed to help organizations support security and compliance needs. While every environment has unique needs, the following PCI Compliance Stack provides a comprehensive mix of VMware solutions with features that are designed to assist with PCI compliance. The solutions' functionality, features, and specific PCI DSS requirements are addressed in detail in the following sections.

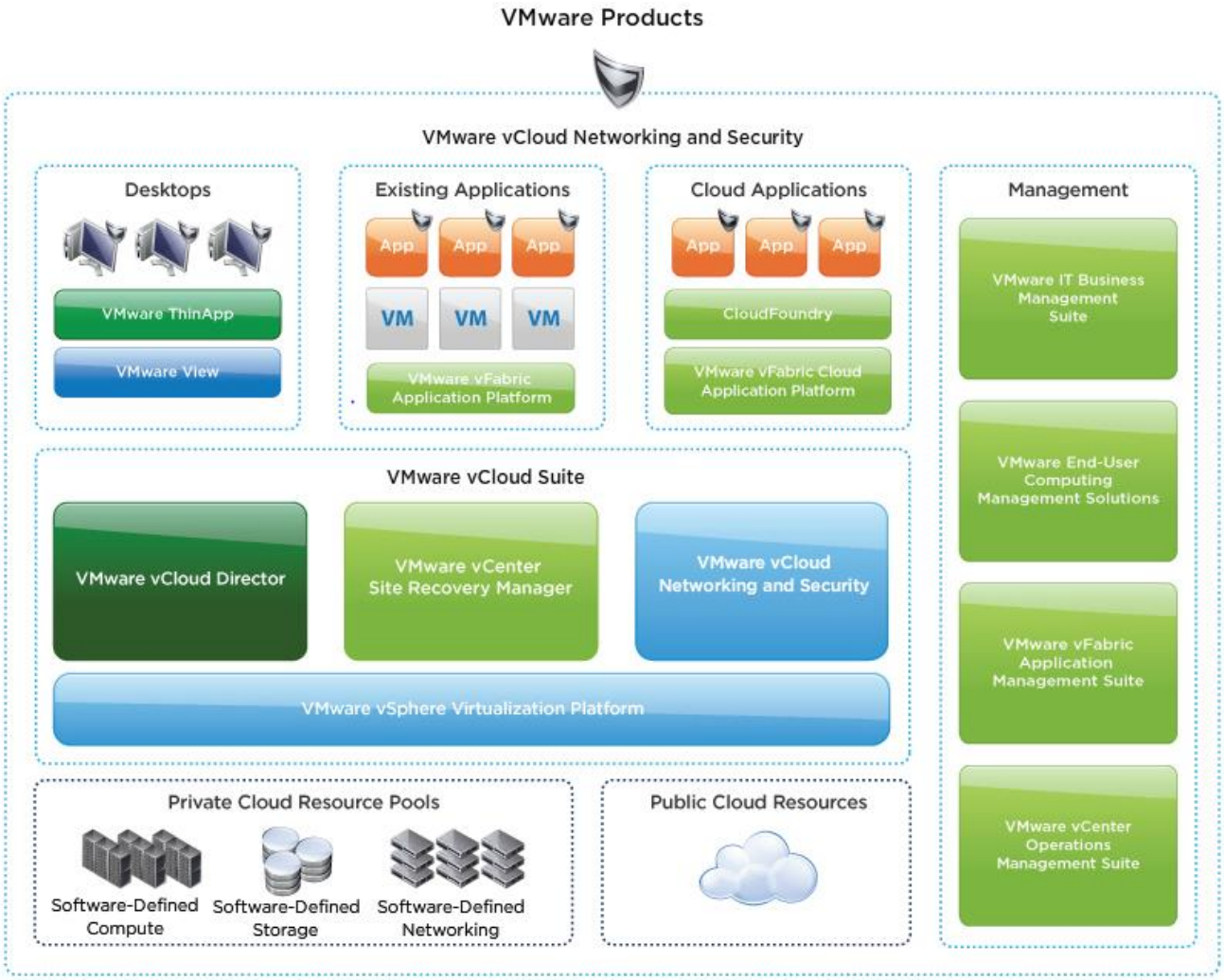
vCloud Suite	ESXi, vShield Endpoint, vCenter Server, vCenter Orchestrator, vCenter Update Manager and vCloud Director
vCloud Networking and Security Suite	Edge Gateway, App, Data Leak Prevention and Manager
vCOPs Suite	vCenter Operations Manager, vCenter Configuration Manager (vCM), vCenter Infrastructure Navigator, and vCenter Chargeback Manager
View Suite	vSphere Desktop, vCenter Server for Desktops, vCenter Desktop, View Manager, ThinApp, View Persona Management, VMware Composer, View Client, vShield Endpoint and View Security Server

To determine the products and features available with VMware Suites please refer to VMware.com:

vCloud Suite 5.1, vCloud Networking and Security Suite 5.1 and vCenter Operations Management Suite

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

Figure 5: VMware Products



VMware PCI Requirements Matrix (Overview)

VMware has created a PCI Requirements Matrix to assist organizations with an understanding of VMware solutions, VMware Partner Solutions (where they overlap), and the remaining customer responsibilities that must be addressed separately by the customer through use of other tools or processes. While every cloud is unique, VMware believes that the vast majority of PCI DSS requirements can be addressed through the VMware Suites and/or VMware partner solutions.

The following diagram shows an example of a cloud environment that has been deployed using the VMware PCI suites and VMware partner products.

The remaining gaps in addressing PCI requirements may be filled by the customer through other tools (i.e. approving customers' policies, keeping an updated network diagram, approving changes, etc.)

Figure 6: Diagrammatic Representation of VMware PCI suites and VMware partner products

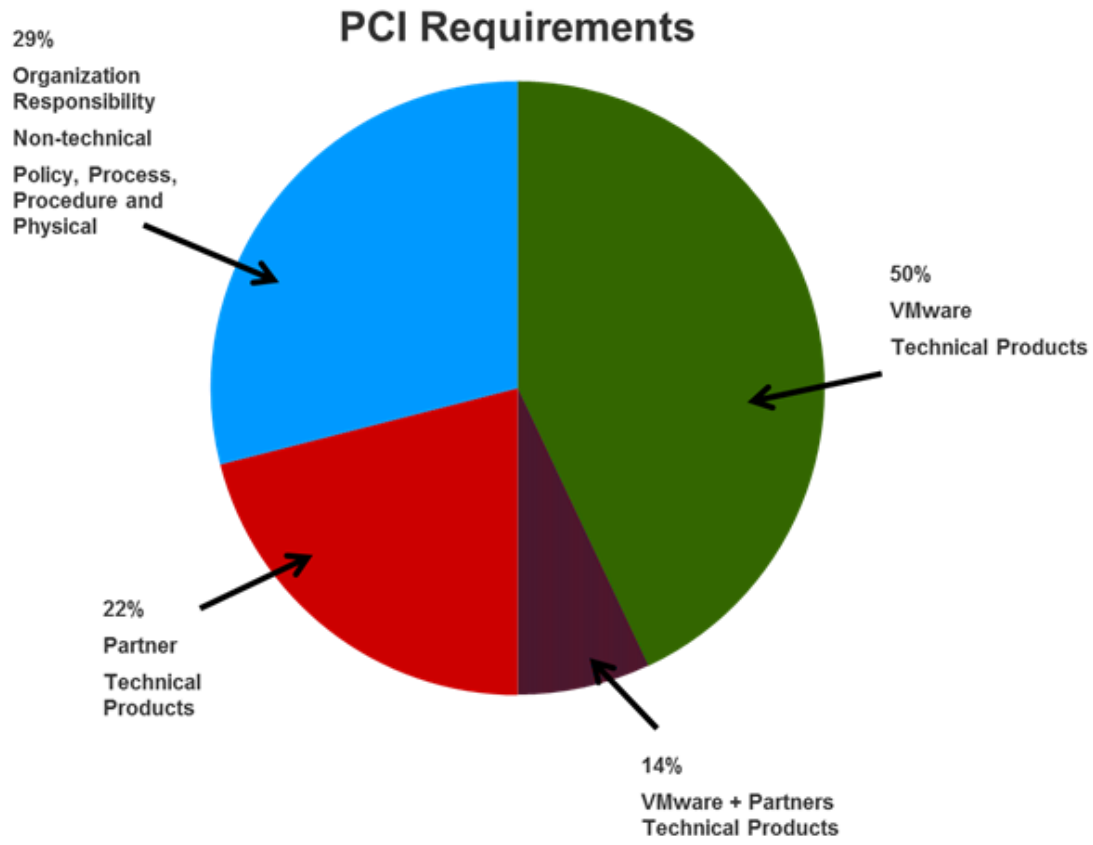


Table 3: PCI DSS Requirement

PIE CHART	PCI DSS REQUIREMENT	# OF PCI ASSESSMENT TESTS	TESTS ADDRESSED IN VMWARE'S SUITES	TESTS ADDRESSED OR ENHANCED BY PARTNERS	TESTS NOT ADDRESSED BY VMWARE OR PARTNERS
	Requirement 1: Install and maintain a firewall configuration to protect cardholder data	25	21	23	2
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	24	23	22	2
	Requirement 3: Protect stored cardholder data	33	12	29	3
	Requirement 4: Encrypt transmission of cardholder data across open, public networks	9	7	9	0
	Requirement 5: Use and regularly update anti-virus software or programs	6	6	6	0
	Requirement 6: Develop and maintain secure systems and applications	32	15	30	2
	Requirement 7: Restrict access to cardholder data by business need to know	7	7	7	1
	Requirement 8: Assign a unique ID to each person with computer access	32	20	30	2
	Requirement 9: Restrict physical access to cardholder data	28	0	0	28
	Requirement 10: Track and monitor all access to network resources and cardholder data	29	27	27	2
	Requirement 11: Regularly test security systems and processes.	24	2	16	8
	Requirement 12: Maintain a policy that addresses the information security for all personnel.	40	1	4	36
	Requirement A.1: Shared hosting providers must protect the cardholder data environment	8	7	7	1
	**TOTAL** **Note: Control totals do not add up to 297 due to overlapping features of VMware products and partner products**	**297**	**148**	**210**	**85**

VMware PCI Requirements Matrix (By VMware Suite)

vCloud Suite

For the purposes of the VMware Solution Guide for PCI, the vCloud Suite includes vSphere (ESXi, vCenter Server), vCenter Orchestrator, vCenter Update Manager and vCloud Director. vSphere provides the foundation of the virtual architecture allowing for the optimization of IT assets. vCloud Director extends the foundation of the vSphere virtual architecture by enabling organizations to build secure clouds and optimizing security and compliance in private, multi-tenant, mixed-mode, and hybrid clouds. As vCloud leverages the vSphere architecture, the vSphere components integrate to create a single vCloud that can be optimized for security and compliance considerations. While it encompasses many features for storage, business continuity, and automation; for the purposes of this PCI reference architecture, the critical components that apply to PCI for vCloud include the following six components – ESXi Hosts, vShield Endpoint, vCenter Server, vCenter Orchestrator, vCenter Update Manager and vCloud Director.

- **ESXi** – ESXi is a type 1 hypervisor (bare metal) that is significantly different than the ESX architecture and offers improvements in security. The ESXi kernel has a small footprint, no service console and can limit communication to vCenter access only. This PCI reference architecture is only applicable to ESXi architectures because the ESXi architecture and the ESX architectures are quite different.

- **vShield Endpoint -** With integration of other 3rd party endpoint solutions (such as anti-virus), vShield Endpoint improves the performance by offloading key antivirus and anti-malware functions to a secured virtual machine and eliminating the antivirus agent footprint and overhead in virtual machines.

- **vCenter Server**—vCenter Server is a server (virtual or physical) that provides unified management for the entire virtual infrastructure and unlocks many key vSphere capabilities. vCenter Server can manage thousands of virtual machines across multiple locations and streamlines administration with features such as rapid provisioning and automated policy enforcement.

- **vCenter Orchestrator** (vCO) – vCO is a virtual appliance that automates tasks for VMware vSphere and enables orchestration between multiple solutions. VMware vCenter Orchestrator allows administrators to automatically create workflows that capture best practices and manual workflows and creates automated, repeatable solutions.

- **vCenter Update Manager** (vUM) – vUM automates tracking, patching and updating for vSphere hosts (ESXi hosts and clusters), VMtools, and VMware virtual appliances. It provides a centralized, automated, actionable patch compliance management solution to confirm that all VMware components are updated and to enforce the latest security patches.

- **vCloud Director (vCD)** - vCD Pools datacenter resources including compute, storage and network, along with their relevant policies into virtual data centers. Fully encapsulated multi-tier virtual machine services are delivered as vApps, using the Open Virtualization Format (OVF). End users and their associated policies are captured in organizations. With programmatic and policy-based pooling of infrastructure, users and services, VMware vCloud Director enforces policies, which enable PCI data to be securely protected, and new virtual machines and applications to be securely provisioned and maintained.

The following product matrix explains which PCI controls are applicable to vCloud. It also explains how vCloud Suite enables users to meet PCI requirements.

Table 4: Applicability of PCI Controls to vSphere

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Segmentation - Though technically not a requirement, segmentation provides a means to reduce the PCI environment and is strongly recommended.	N/A	The vCloud Suite can be configured to limit access to the Cardholder Data Environment (CDE) through a variety of ways. By providing a centralized interface, vSphere Client and vCenter servers can reduce the CDE by minimizing the network management and limiting access to critical components in the CDE. Controlling and limiting the access and administrative abilities for users managing a vCloud environment reduce PCI Scope. This helps to provide the transparency of data flows, network communication, and configuration settings for critical components within the CDE. vCloud Director and vCenter Server can be used to demonstrate the scope that is being enforced by analyzing and reporting data flows between various components and network devices (such as relationships between databases, virtual appliances, VM's, hosts, etc). The ESXi host is a type 1 hypervisor (bare metal) that limits the attack vectors. By reducing the complexities of the hypervisor, companies and their auditors can better understand the risks to virtual environments.For example, the vSphere environment allows users to lock down each ESXi server so that it can only be accessed via the vCenter server. vCO can also be used to automate and enforce standardized rules, accounts, profiles, and security settings in order that scope is not impacted as new machines are dynamically added or removed. Specifically, vCO can be used to configure new virtual components to communicate only within the environment in which they were intended. vCO can reduce the manual configuration processes which are prone to user error and misconfiguration in a large, dynamic environment.
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1.1, 1.1.2a, 1.1.2.b, 1.1.4, 1.1.5a, 1.1.5.b, 1.2.1a, 1.2.1.b, , 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 1.3.8a, 1.3.8.b	The vCloud environment enforces a centralized process through the vCenter Server that can be used to enforce formal processes for making changes to the network. vCenter Server, along with ESXi host establishes and enforces communication between the virtual machines at layer 2 level. The vSphere architecture takes many functions normally handled by physical switching appliances and establishes virtual switches (vS), distributed virtual switches (dvS), Port Groups, VLAN's, Management Interfaces, etc. The vCloud and vSphere architectures allows administrators to establish formal processes for approving network changes and provides maps and data flows that allow for greater visibility into the relationships between ESXi hosts, storage, virtual machines, virtual switches, virtual appliances, and vApps. The integration of the vCloud Networking and Security Suite provides central visibility into open ports, services, and protocols is designed to allow only approved traffic into and out of the cardholder data environment. vCO can assist with automation of many manual processes which are prone to human error in a traditional hardware based environment, thereby ensuring that every change to the CDE is enforced through pre-approved templates, workflows, and administrators.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.1.1.a, 2.1.1.c, 2.1.1.d, 2.1.1.e, 2.2.a, 2.2.b, 2.2.c, 2.2.d, 2.2.1.a, 2.2.1.b, 2.2.2.a, 2.2.2.b,	Changing vendor-supplied default passwords is a challenge in large distributed environments. vCO can automate the provisioning process to provide that all components in the vSphere infrastructure are built to a known security baseline and vendor settings are re-set. Additionally, direct access to components can be reduced (such as lock-down mode) to minimize the risk of any direct console or shell access. vUM can be used to push out critical security updates that allow the latest security configurations to be enforced.

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
	2.2.3.b, 2.2.3.c, 2.2.4.a, 2.2.4.b, 2.2.4.c, 2.3.a, 2.3.b, 2.3.c, 2.4	Integrating into vSphere components such as vUM, the vCloud Director environment can be used to push out critical security updates to enable the latest security configurations to be enforced. Hardening guidelines have been developed specifically for the Cloud environment (such as the VMware® vCloud Director 1.5 DIACAP Implementation Plan). vCloud Director and vSphere provide centralized views to make sure that only necessary ports and protocols are being used. vCloud can enforce strong remote access to components by enforcing secure remote access such as SSH, IPsec or SSL, or it can be used to disable direct access and force administration through centralized vSphere processes. For shared hosting providers, different administrative groups can be enforced to protect each hosted entity through the establishment of RBAC, groups, data centers, and other pools.
Requirement 3: Protect stored cardholder data	3.1.1.d, 3.1.1.e, 3.2.a,	vSphere can be used to establish and enforce automated procedures designed to prevent virtual machines in the CDE from being retained for longer than required. This is achieved by providing a centralized process for deleting old vm's and snapshots. When a virtual machine or snapshot is no longer necessary, access to that system can be permanently revoked.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	N/A	N/A
Requirement 5: Use and regularly update anti-virus software or programs	5.1, 5.1.1, 5.2.a, 5.2.b, 5.2.c, 5.2.d,	vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. It is designed to leverage existing Endpoint investments by allowing organizations to manage antivirus and anti-malware policies for virtualized environments with the same management interfaces they use to secure physical environments. It establishes an API, which allows for the integration of third party anti-virus solutions. These solutions can run unique endpoint operations such as conducting anti-virus scanning for systems that are offline or agentless anti-virus. Endpoint provides a centralized solution that allows the user to verify that anti-virus is installed on all applicable hosts, actively running, and logging.
Requirement 6: Develop and maintain secure systems and applications	6.1.a, 6.1.b, 6.4.1, 6.4.2, 6.4.4, 6.4.5.a,	vUM provides a centralized solution designed to confirm that all system components are patched and running on the most recent versions. Patches can be manually deployed or automatically pushed out through a combination of vUM and vCO. vSphere provides visibility into separate test and development networks and users, and can be used so that access between the development and products networks do not use similar networks or administrative accounts for virtual components.
Requirement 7: Restrict access to cardholder data by business need to know	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3	vCloud and vSphere have built in access control systems in place so that each virtual component can only be accessed by authorized users. Systems can be accessed directly with local accounts, or can be managed centrally through a role based access control systems enforced by vSphere and integrated into centralized access control system.
Requirement 8: Assign a unique ID to each person with computer access	8.1, 8.2, 8.4.a, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6.a, 8.5.6.b,	All access to virtual devices within the vCloud and vSphere environment can enforce individual access. Minimum usernames and password requirements can be set on many systems natively (such as the ESXi host). Other virtual components can be configured to use centralized authentication servers (such as

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
	8.5.8.a, 8.5.8.b, 8.5.8.c, 8.5.9.a, 8.5.9.b, 8.5.10.a, 8.5.10.b, 8.5.11.a , 8.5.12.a, 8.5.13.a, 8.5.14, 8.5.15	Active Directory) which can enforce additional controls for password rotation, lockout, duration etc.
Requirement 9: Restrict physical access to cardholder data	N/A	N/A
Requirement 10: Track and monitor all access to network resources and cardholder data	10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.a, 10.4.1.a, 10.4.1.b, 10.4.2.a, 10.4.2.b, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.7.a, 10.7.b	vCloud and vSphere has the ability to log access to components within the environment. Individual access to components can be tracked, logged, and enforced. Audit trails can capture event, time, action, and other critical requirements that are required for monitoring. Logs can be centrally consolidated, reviewed, and retained for analysis. All systems can be configured with time synchronization, normally by enforcing primary and secondary NTP servers in the cloud environment.
Requirement 11: Regularly test security systems and processes.	N/A	N/A
Requirement 12: Maintain a policy that addresses information security for all personnel.	12.2	vCO can be used to automate and enforce daily operational security procedures.
Requirement A.1: Shared hosting providers must protect the cardholder data environment.	A.1.1, A.1.2.a, A.1.2.b, A.1.2.c, A.1.2.d, A.1.2.e, A.1.3.	vSphere has the ability to log access to components within the vSphere environment. Individual access to components can be tracked, logged, and enforced. Audit trails can capture event, time, action, and other critical requirements that are required for monitoring. Logs can be centrally consolidated, reviewed, and retained for analysis. All systems can be configured with time synchronization, normally by enforcing primary and secondary NTP servers in the vSphere environment. Changing vendor-supplied default passwords is a challenge in large distributed environments. vCloud Director can automate the provisioning process so that all components in the cloud infrastructure are built to a known security baseline and vendor settings are re-set. Additionally, direct access to components can be reduced (such as lock-down mode) to minimize the risk of any direct console or shell access. Integrating into vSphere components such as vUM, Clouds using the vCloud Director environment can be used to push out critical security updates to allow the latest security configurations to be enforced. Hardening guidelines have been developed specifically for the Cloud environment (such as the VMware®

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
		vCloud Director 1.5 DIACAP Implementation Plan). vCD provide a centralized view designed to confirm that only necessary ports and protocols are being used. vClouds can enforce strong remote access to components by enforcing secure remote access such as SSH or SSL, or it can be used to disable direct access and force administration through centralized processes. For shared hosting providers, different administrative groups can be enforced to protect each hosted entity through the establishment of RBAC, groups, data centers, and other pools.

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

vCloud Networking and Security Suite

For the purposes of the VMware Solution Guide for PCI, the suite is a group of products that deliver a virtualized security model specifically designed to overcome the traditional challenges of managing security in a virtual environment. vCloud Networking and Security provides a software based approach to application and data security in virtual and cloud environments, which have traditionally been enforced primarily through physical security appliances. The vCloud Networking and Security suite consists of the following five (5) products:

- **App**
  Protects applications in a virtual datacenter against network-based threats by providing a firewall that is hypervisor-based and application-aware. vCloud Networking and Security App has visibility of intra-VM communication, and enforces policies, firewall rules based on logical groups, and workloads.

- **Data Leak Prevention**
  Adds to Sensitive Data Discovery across virtualized resources allowing the organizations to identify and secure different types of sensitive data. For PCI, it provides a way to search for cardholder data and to identify hosts and unauthorized stores of data.

- **Edge Gateway**
  Enhances protection of a virtual datacenter perimeter by providing gateway security services including careful inspection firewall, site-to-site VPN, load balancing, Dynamic Host Configuration Protocol (DHCP), and Network Address Translation (NAT). It also has the ability to integrate with third-party IDS solutions.

- **Manager**
  Manager is a management application, which includes all vCloud Networking and Security products. Manager is tightly integrated with vCenter and the broader VMware management portfolio.

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

The following product matrix explains which PCI controls are applicable to the vCloud Networking and Security Suite. It also explains how vCloud Networking and Security assists users in meeting PCI requirements.

Table 5: PCI DSS v2.0 Applicability Matrix

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Segmentation - While technically not a requirement, segmentation provides a means to reduce the risk to a PCI environment and is strongly recommended.	N/A	vCloud Networking and Security can provide segmentation for Cloud environments by segmenting virtual machines, port groups, and enforcing perimeter security. Edge gateway provides gateway security services including a stateful inspection firewall, which protects the network from traffic into and out of the virtualized infrastructure. App provides visibility and control for intra-VM communication. Data Leak Prevention can be used to proactively search and identify stores of credit card data and gather data to validate or enforce segmentation.
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1.1, 1.1.2a, 1.1.2.b, 1.1.4, 1.1.5.a, 1.1.5.b, 1.2.1.a, 1.2.1.b, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8.a, 1.3.8.b	vCloud Networking and Security Manager provides centralized management and can be used to enforce the approval process for changes to network connections. Edge Gateway and App can control how cardholder data flows over a network, and Data Leak Prevention can be used to monitor that those controls are operating effectively. Roles and responsibilities for management can be enforced and defined in Manager and integrated into other RBAC solutions. Edge Gateway can be used as a firewall to separate wireless networks from the virtual infrastructure. Both Edge Gateway and App perform stateful inspection (dynamic filtering). App and Edge Gateway also support comment fields, which can used to document the justification for every open port and service. Manager can be used to view current configurations and allow an administrator to compare it to an approved configuration; This facilitates confirmation that running configurations files for App and Edge Gateway are secured and match the approved configurations.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.1.1.a, 2.1.1.c, 2.1.1.d, 2.1.1.e, 2.2.a, 2.2.b, 2.2.c, 2.2.d, 2.2.1.a, 2.2.1.b, 2.2.2.a, 2.2.2.b, 2.2.3.b, 2.2.3.c, 2.2.4.a, 2.2.4.b, 2.2.4.c, 2.3.a, 2.3.b, 2.3.c, 2.4	vCloud Networking and Security has published hardening guidelines, installation guidelines, configuration guidance, and/or other implementation procedures which enable organizations to ascertain that they have deployed App, Edge Gateway, Manager, and Data Leak Prevention in a secured manner. vCloud Networking and Security supports secured remote access (SSH and SSL).
Requirement 3: Protect stored cardholder data	3.1.1.a, 3.1.1.b, 3.1.1.c, 3.1.1.d, 3.1.1.e, 3.2.a, 3.2.1, 3.2.2, 3.2.3, 3.4.a, 3.4.b, 3.4.d,	vCloud Networking and Security Data Leak Prevention can programmatically identify and quarantine stored cardholder data that exceeds business requirements or data retention policies. For example, if a system is scanned and Primary Account Numbers (PAN) are identified, rules can be established which move the VM to the PCI CDE or to quarantine area for further review. It can also be used to verify that cardholder data is not stored in violation of the organization policies. In addition to PAN searches, it can be used to search for and identify sensitive authentication data for organization that needs to store sensitive authentication data (such as issuers).
Requirement 4: Encrypt	4.1, 4.1.a, 4.1.b, 4.1.c,	vCloud Networking and Security Edge Gateway can be used to secure data transmitted over open-public

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
transmission of cardholder data across open, public networks	4.1.d, 4.1.e,	networks by establishing IPsec VPN's between data centers which are connected over public networks.
Requirement 5: Use and regularly update anti-virus software or programs	NA	NA
Requirement 6: Develop and maintain secure systems and applications	6.1.a, 6.1.b, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5.a	Patches for the vCloud Networking and Security Suite of products can be automatically detected through the vSphere architecture using vUM. These patches are pushed to virtual components to confirm that vCloud Networking and Security components are running on the latest versions. The vCloud Networking and Security Suite can be utilized to determine that test, development, and production systems are properly segmented and are not using live PAN data through the use of App with Data Leak Prevention.
Requirement 7: Restrict access to cardholder data by business need to know	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3	vCloud Networking and Security supports authentication based on job classification and function (RBAC), and can be configured to require that only the appropriate administrators and support personnel have access to vCloud Networking and Security components and operations. Manager provides a centralized solution to manage and enforce security profiles across a large distributed environment.
Requirement 8: Assign a unique ID to each person with computer access	8.1, 8.2, 8.4.a, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6.a, 8.5.6.b, 8.5.8.a, 8.5.8.b, 8.5.9.a, 8.5.9.b, 8.5.10.a, 8.5.10.b, 8.5.11.a, 8.5.12.a, 8.5.13.a, 8.5.14, 8.5.15.a	The vCloud Networking and Security Suite along with Manager can be configured to support centralized authentication solutions through vCenter which can enforce unique ID's, passwords, reset automatically for first-time log-ins, automatically disables old accounts, minimum length, complexity, re-use, lock out attempts, lockout durations, and session idle time.
Requirement 9: Restrict physical access to cardholder data	N/A	N/A
Requirement 10: Track and monitor all access to network resources and cardholder data	10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.a, 10.4.1.a, 10.4.1.b, 10.4.2.a, 10.4.2.b, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.7.a, 10.7.b	vCloud Networking and Security App and Edge Gateway have the ability to log access to components within the virtual environment using Syslog. Individual access to components can be tracked, logged, and enforced. Audit trails can capture event, time, action, and other critical requirements required for monitoring. Logs can be centrally consolidated, reviewed, and retained for analysis. All systems can be configured with time synchronization, normally by enforcing primary and secondary NTP servers in the vSphere environment.
Requirement 11: Regularly test security systems and processes.	11.4.a, 11.4.b, 11.4.c	vCloud Networking and Security Edge Gateway can be integrated into third party for Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS).

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Requirement 12: Maintain a policy that addresses information security for all personnel.	12.2	vCloud Networking and Security can be used to automate and enforce daily operational security procedures.
Requirement A.1: Shared hosting providers must protect the cardholder data environment.	A.1.1, A.1.2.a, A.1.2.b, A.1.2.c, A.1.2.d, A.1.2.e, A.1.3.	vCloud Networking and Security has published hardening guidelines, installation guidelines, configuration guidance, and/or other implementation procedures which enable organizations to confirm that they have deployed App, Edge Gateway, Manager, and Data Leak Prevention in a secured manner. vCloud Networking and Security supports secured remote access (SSH and SSL).

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

vCenter Operations Management Suite

For the purpose of the VMware Solution Guide for PCI, the "vCenter Operations Management Suite" includes vCenter Operations Manager, vCenter Configuration Manager, vCenter Infrastructure, and vCenter Chargeback Manager. The vCenter Operations Management Suite enables IT organizations to gain better visibility and actionable intelligence to proactively facilitate service levels, optimum resource usage, and configuration compliance in dynamic virtual and cloud environments.

- **vCenter Operations Manager (vCOPs)** – Uses patented analytics and integrated approach to operations management in order to provide the intelligence and visibility required to proactively maintain service levels, optimum resource usage, and configuration compliance in dynamic virtual and cloud environments.

- **vCenter Configuration Manager** (vCM) – Automates configuration management across virtual and physical servers and desktops, increasing efficiency by eliminating manual, error-prone, and time-consuming work. This enables enterprises to maintain continuous compliance by detecting changes and comparing them to configuration and security policies.

- **vCenter Infrastructure Navigator** – Automatically discovers and visualizes application and infrastructure dependencies. It provides visibility into the application services running over the virtual-machine infrastructure and their interrelationships for day-to-day operational management.

- **vCenter Chargeback Manager** – Enables accurate cost measurement, analysis and reporting of virtual machines, and provides visibility into the actual cost of the virtual infrastructure required to support business services.

The following product matrix explains which PCI controls are applicable to the vCenter Operations Management (vCOPs) Suite. For the purpose of VMware Solution Guide for PCI, vCenter Configuration Manager (vCM) is the principal application within the vCOPs Suite that allows it to help the user meet PCI compliance standards. The following is the detailed description of the controls that may be met through the Suite.

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

Table 6: PCI DSS v2.0 Applicability Matrix

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Segmentation - While technically not a requirement, segmentation provides a means to reduce the PCI environment and is strongly recommended.	N/A	N/A
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1.1, 1.1.2.a, 1.1.2.b, 1.1.4, 1.1.5.a, 1.1.5.b, 1.2.1.b, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 1.3.8.a, 1.3.8.b,	N/A
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.1.1.a, 2.1.1.c, 2.1.1.d, 2.1.1.e, 2.2.a, 2.2.b, 2.2.c, 2.2.d, 2.2.1.a, 2.2.1,b, 2.2.2.a, 2.2.2.b, 2.2.3.b, 2.2.4.a, 2.2.4.b, 2.2.4.c, 2.3.a, 2.3.b, 2.3.c, 2.4	Security hardening and the enforcement of configuration standards are difficult in any environment and have historically relied on manual processes. The vCOPs suite has the ability to assess both physical and virtual machines in the CDE and report their compliance with a variety of configuration concerns. vCOPs has the ability to consistently check the compliance status of machines within the environment critical for the configuration management and hardening of systems. Items such as default system settings, system security hardening and base-lining, un-provision and unapproved software or services, and report unnecessary functions from systems. vCOPs allows the customer to customize any number of compliance templates created to meet regulatory and best practices standards including, but not limited to CIS, ISO-27001/27002, SANS and NIST. This function will allow for the simple baseline of standards and security configuration.
Requirement 3: Protect stored cardholder data	3.1.1.d, 3.1.1.e, 3.2.a	N/A
Requirement 4: Encrypt transmission of cardholder data across open, public networks	N/A	N/A
Requirement 5: Use and regularly update anti-virus software or programs	5.1, 5.1.1., 5.2.a, 5.2.b, 5.2.c, 5.2.d	vCOPs does not have a built in anti-virus solution, but it can be used to asses and report the anti-virus state of the systems. This allows a determination that all systems have anti-virus software installed and running with the updated signature files. vCOPs can remediate anti-virus problems by installing the customer approved anti-virus software on systems where it is not installed starting/enabling the software services.
Requirement 6: Develop	6.1.a, 6.1.b, 6.4.1,	vCOPs with VCM is able to assess, download, and deploy patches to Windows, Unix, Linux, and MAC

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
and maintain secure systems and applications	6.4.2, 6.4.4, 6.4.5.a, 6.4.5.1, 6.4.5.2, 6.4.5.3.a, 6.4.5.3.b, 6.4.5.4	operating systems. Assessments are customizable and can be set to verify critical patches in the past 30 days. Changes within the virtual environment are captured by vCOPs. Each change made to the configuration settings is documented and logged. If a change is made without the proper approval it is alerted with a simple roll back procedure and the change is reversed. vCOPs are able to track changes both made through the standard change process or out of band changes conducted directly on the VMs or through another tool.
Requirement 7: Restrict access to cardholder data by business need to know	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3	Access to vCOPs can be controlled through Microsoft Active Directory. This will allow vCOPs to helo the user meet the PCI requirements for access control to the CDE.
Requirement 8: Assign a unique ID to each person with computer access	8.1, 8.2, 8.4.a, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6.a, 8.5.6.b, 8.5.8.a, 8.5.8.b, 8.5.9.a, 8.5.9.b,8.5.10.a, 8.5.10.b, 8.5.11.a, 8.5.12.a, 8.5.13, 8.5.14, 8.5.15	vCOPs has the ability to monitor access controls to the CDE and thereby monitor compliance with PCI DSS requirements. Specifically, vCOPs will assess and report on the following: - Local and domain-level users (Windows) and users with unique usernames (UNIX, Linux and MAC OS). - System password policies for expiration, length, standards, creation settings, access attempts, (can also remediate) - Changes to user accounts, credential stores, and identifier objects to provide visibility and control over system access - User access across all the systems in the datacenter at once - Disable and remove access for terminated user accounts - Inactive accounts (which it can also disable and remove access for these user accounts) - The status of maintenance accounts and to confirm that they are disabled and configured to only be used during the times specified. - Login policies, to include lockout settings and auto-logout settings, and remediating as needed. Assessment, reporting and remediation is conducted in accordance with scheduling through vCOPs.
Requirement 9: Restrict physical access to cardholder data	N/A	N/A
Requirement 10: Track and monitor all access to network resources and cardholder data	10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.a, 10.4.1.a, 10.4.1.b, 10.4.2.a, 10.4.2.b, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5,	vCOPs will assess, report and remediate the following: - Configurations of the system auditing and logging services to support proper logging across system components. - vCM collects audit log entries to provide a single view of events. - NTP settings and configuration details. - User access audit trails by ensuring proper permissions for log files and their directories and alert on changes to critical audit trails. vCOPs has the ability to track system changes across thousands of data points and, in conjunction with

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
	10.7.a, 10.7.b,	native auditing, can be used to track account activity and system modifications. vCOPs can assess and report on Syslog configuration details on Unix and Linux systems that specify remote log servers within the network.
Requirement 11: Regularly test security systems and processes.	N/A	vCOPs can perform file integrity monitoring (FIM) within the CDE for critical files and/or directories. Alerts can also be established to alert personnel of any changes made or attempted and even remediate as needed. This ability allows vCOPs to enable the user to meet the PCI DSS requirements for FIM.
Requirement 12: Maintain a policy that addresses information security for all personnel.	12.2	vCOPs can be used to automate and enforce daily operational security procedures.
Requirement A.1: Shared hosting providers must protect the cardholder data environment.	A.1.3.	vCOPs will assess, report and remediate the following: - Configurations of the system auditing and logging services to support proper logging across system components. - vCM collects audit log entries to provide a single view of events. - NTP settings and configuration details. - User access audit trails by providing proper permissions for log files and their directories and alert on changes to critical audit trails. vCOPs has the ability to track system changes across thousands of data points and, in conjunction with native auditing, can be used to track account activity and system modifications. vCOPs can assess and report on Syslog configuration details on Unix and Linux systems that specify remote log servers within the network.

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

View Suite

For the purposes of the VMware Solution Guide for PCI, the "View" suite of products includes VMware vSphere Desktop, VMware vCenter Server for Desktops, vCenter Desktop, VMware View Manager, VMware ThinApp, VMware View Persona Management, VMware Composer, VMware View Client, VMware vShield Endpoint, and View Security Server. View provides the foundation of the virtual architecture allowing for the optimization of IT assets.

- **VMware vSphere Desktop**
  The vSphere Desktop product is a version of vSphere specifically licensed for a View deployment. The vSphere Desktop product consists of the ESXi hypervisor and numerous features to maximize the efficiency and security of multiple ESXi hosts, plus vCenter.

- **VMware vCenter Server for Desktops**
  This edition of VMware vCenter™ Server is the central management hub for VMware vSphere and gives the complete control and visibility over clusters, hosts, virtual machines, storage, networking and other critical elements of the virtual infrastructure.

- **vCenter Desktop**
  The vCenter Desktop product is a required component for VMware View. It manages the virtual machines within the ESX hosts. The vCenter Desktop product is the version of vCenter that is bundled with View.

- **VMware View Manager (sometimes referred to as View Administrator)**
  View Administrator is a web-based application that is installed when you install View Connection Server. It is the management interface for View Connection Server. Administrators use View Administrator to configure the View Connection Server, to deploy and manage desktops, to control user authentication, to initiate and examine system events, and to carry out analytical activities. View Administrator is also used to manage security servers and the View Transfer Server instances associated with View Connection Server.

- **VMware ThinApp**
  VMware ThinApp™ is an agentless application virtualization solution that streamlines application delivery while eliminating conflicts. As part of VMware View, ThinApp simplifies repetitive administrative tasks and reduces storage needs for virtual desktops by maintaining applications independently from the underlying OS.

- **VMware View Persona Management**
  View Persona Management provides persistent, dynamic user profiles across user sessions on different desktops. The user profile data is downloaded as needed to speed up login and logout time, and new user settings are sent up to the user profile repository automatically during desktop use.

  Persona Management is an optional component included with View Premier.

- **VMware Composer**
  VMware View Composer lets customers easily manage pools of "like" desktops by creating gold master images that share a common virtual disk. All cloned desktops linked to a master image can be patched or updated through VMware View Manager by simply updating the single master image, without affecting users' settings, data or applications.

- **VMware View Client**
  View Client enables access to centrally host virtual desktops from Windows PCs, Macs, thin clients, zero clients, iPads, and Android-based clients. View Client with Local Mode allows access to virtual desktops running on a local Windows based endpoint regardless of network availability.

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

- **vShield Endpoint**
  vShield Endpoint can be integrated into an environment using View and managed through other VMware solutions such as vCloud Networking and Security Manager and partner solutions designed for the VMware architecture. vShield Endpoint utilizes third party endpoint solutions to perform unique functions such as offloading and centralizing anti-virus and anti-malware (AV) solutions. This integration strongly decreases AV storm issues, minimizes the risk of malware infection, and simplifies AV administration. vShield Endpoint relieves virtual machines of the burden of defending against viruses and malware.

- **View Security Server**
  View Security Server provides an extra layer of security for external Internet users connecting to a View Connection Server to access the internal network. The Security Server handles SSL functions.

The following product matrix explains which PCI controls are applicable to View and how the View product assists users with meeting PCI requirements.

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

Table 7: PCI DSS v2.0 Applicability Matrix

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Segmentation - While technically not a requirement, segmentation provides a means to reduce the PCI environment and is strongly recommended.	N/A	VMware View assists by taking the computing endpoints out of scope to a certain extent by minimizing transmission of actual protected data except in the form of display protocol. When configured correctly, no data will be saved on the hardware of the device and can be used to reduce the scope and impact of virtual terminals. If integrated with Point to Point Encryption (P2PE), View has the potential to completely remove the virtual terminal PC from scope.
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	1.1.3.a, 1.1.3.b, 1.2.1.a, 1.2.1.b, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 1.3.8.a, 1.3.8.b,	VMware View provides its own Security Server, an HTTPS proxy which lives typically in a DMZ and brokers connection of the client to the display protocol driver in the virtual machine. The Security Server uses a default deny policy and must be explicitly configured to connect with a connection server to allow external traffic to reach the internal network. In addition, vCloud Networking and Security Edge Gateway can be utilized to segment the View network from the external network.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	2.1, 2.1.1.a, 2.1.1.c, 2.1.1.d, 2.1.1.e, 2.2.a, 2.2.b, 2.2.c, 2.2.2.a, 2.2.2.b, 2.2.3.b, 2.2.3.c, 2.2.4.a, 2.3.a, 2.3.b, 2.3.c, 2.4	VMware View relies entirely on Active Directory credentials and stores links as foreign security principals in its own LDAP (AD LDS).
Requirement 3: Protect stored cardholder data.	N/A	Since VMware View displays data as pixels and relies on vSphere and other VMware infrastructure for storing desktop OS images it would defer to those capabilities to meet that requirement. While VMware View has an 'Offline Mode' capability that would require some whole disk encryption and other controls this would not be utilized for in a PCI compliant environment.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.	4.1 , 4.1.a, 4.1.b, 4.1.c, 4.1.d, 4.1.e, 4.1.1	VMware View uses PCoIP for software and hardware ("zero" clients) that natively uses an encrypted protocol. PCoIP compresses, encrypted, and encoded data and provides a "pixels only" view for the end user.
Requirement 5: Use and regularly update anti-virus software or programs.	5.1, 5.1.1, 5.2.a, 5.2.b, 5.2.c, 5.2.d	View relies upon vShield Endpoint designed to work with View for protection/remediation. vShield Endpoint is the solution to the problems inherent in antivirus scanning in a large-scale virtual desktop implementation. In a VMware View environment, vShield Endpoint consolidates and offloads two antivirus operations into one centralized virtual appliance: • Checking for virus signature update files

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
		• Antivirus scanning VMware has partnered with antivirus software vendors to provide this bundled solution to antivirus problems in the VDI environment. VMware partners supply a dedicated, secure virtual appliance. This virtual appliance integrates with vShield Endpoint APIs to protect VMware virtual desktops against viruses and other malware. Instead of installing antivirus agents on each virtual desktop, you can connect one virtual appliance to each virtual machine host.
Requirement 6: Develop and maintain secure systems and applications.	6.1.a, 6.1.b	View relies upon associated VMware products separate from the View Suite for security updates. VMware Update Manager (vUM) is utilized for all VMware components and Shavlik for guest VMs.
Requirement 7: Restrict access to cardholder data by business need to know.	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3	View integrates with third party software (Microsoft Active Directory) to provide role based access control that is designed to meet PCI DSS requirements. Additionally, View may enable two-factor authentication to help the user meet the requirements for remote access to the View environment.
Requirement 8: Assign a unique ID to each person with computer access.	8.1, 8.2, 8.4.a, 8.5.1, 8.5.3, 8.5.4, 8.5.5, 8.5.6.a, 8.5.6.b, 8.5.8.a, 8.5.8.b, 8.5.9.a, 8.5.9.b, 8.5.10.a, 8.5.10.b, 8.5.11.a, 8.5.12.a, 8.5.13.a, 8.5.14, 8.5.15	View integrates with Microsoft Active Directory to provide role based access control. Additionally, View may enable RSA SecureID connections for two-factor authentication.
Requirement 9: Restrict physical access to cardholder data.	N/A	N/A
Requirement 10: Track and monitor all access to network resources and cardholder data.	10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.a, 10.4.1.a, 10.4.1.b, 10.4.2.a, 10.4.2.b, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.7.a, 10.7.b	View allows logging to be captured in accordance with PCI DSS requirements with third party products. Structured text logs and other logging from supporting applications Microsoft Active Directory, AD LDS and SQL Server can all be utilized to meet the control requirements.
Requirement 11: Regularly test security systems and processes.	N/A	N/A

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

PCI DSS V2.0 APPLICABILITY MATRIX		
REQUIREMENT	**CONTROLS ADDRESSED**	**DESCRIPTION**
Requirement 12: Maintain a policy that addresses information security for all personnel.	12.2	View can be used to automate and enforce daily operational security procedures.
Requirement A.1: Shared hosting providers must protect the cardholder data environment.	A.1.3.	View allows logging to be captured in accordance with PCI DSS requirements with third party products. Structured text logs and other logging from supporting applications Microsoft Active Directory, AD LDS and SQL Server can all be utilized to assist in meeting the control requirements.

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

Detailed PCI Applicability Matrix for VMware and VMware Partners

Table 8: PCI Applicability Matrix for VMware Partners

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.1 Establish firewall and router configuration standards that include the following:	1.1 Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:											
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	✓	✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	✓	✓	✓								
	1.1.2. b Verify that the diagram is kept current.	✓	✓	✓								
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	1.1.3 a Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.		✓		✓							
	1.1.3. b Verify that the current network diagram is consistent with the firewall configuration standards.			✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.	1.1.4 Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.	✓	✓	✓								
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	1.1.5.a Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	✓	✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.	✓	✓	✓								
1.1.6 Requirement to review firewall and router rule sets at least every six months.	1.1.6.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.											
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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 Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:											
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	1.2.1.a Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	✓	✓		✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit —deny allll or an implicit deny after allow statement.	✓	✓	✓	✓							
1.2.2 Secure and synchronize router configuration files.	1.2.2 Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.				✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	1.2.3 Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.		✓									

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.											
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	1.3.1 Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	1.3.2 Verify that inbound Internet traffic is limited to IP addresses within the DMZ.		✓	✓								
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	1.3.3 Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.		✓	✓								
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	1.3.4 Verify that internal addresses cannot pass from the Internet into the DMZ.		✓	✓								
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only —established‖ connections are allowed into the network.)	1.3.6 Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)		✓									
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other non- trusted networks.	1.3.7 Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other non-trusted networks.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.3.8 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 or content caches, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.	1.3.8.a Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.		✓									
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	1.4.a Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.											
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
2.1 Always change vendor-supplied default settings before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	2.1 Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			✓								
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change	2.1.1 Verify the following regarding vendor default settings for wireless environments:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions			✓								
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.			✓								
	2.1.1.c Verify default passwords/passphrases on access points were changed.			✓								
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.			✓								

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.			✓								
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)	2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	✓		✓	✓							
	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.	✓		✓	✓							
	2.2.c Verify that system configuration standards are applied when new systems are configured.	✓		✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).	✓		✓	✓							
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	2.2.1.a For a sample of system components, verify that only one primary function is implemented per server.	✓		✓								
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.	✓		✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	2.2.2.a For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.	✓	✓	✓	✓							
	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
2.2.3 Configure system security parameters to prevent misuse.	2.2.3.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.											
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.	✓	✓	✓	✓							
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	✓	✓	✓	✓							
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	2.2.4.a For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	✓		✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	2.2.4.b. Verify enabled functions are documented and support secure configuration.	✓	✓	✓	✓							
	2.2.4.c. Verify that only documented functionality is present on the sampled system components.	✓	✓	✓	✓							
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	2.3 For a sample of system components, verify that non-console administrative access is encrypted by performing the following:											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.	✓	✓	✓	✓							
	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.	✓	✓	✓	✓							
	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	2.4 Perform testing procedures A.1.1 through A.1.4 detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	✓	✓	✓	✓							
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	3.1 Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.1.1 Implement a data retention and disposal policy that includes: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. • Processes for secure deletion of data when no longer needed. • Specific retention requirements for cardholder data. • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	3.1.1.a Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).		✓	✓								
	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.		✓	✓								
	3.1.1.d Verify that policies and procedures include at least one of the following: § A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy • Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.		✓									
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: Note: 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.	3.2.a For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.		✓									
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	3.2.c For each item of sensitive authentication data below, perform the following steps:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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). 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.	3.2.1 For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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.	3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	3.2.3 For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:• Incoming transaction data• All logs (for example, transaction, history, debugging, error)• History files• Trace files• Several database schemas• Database contents		✓	✓								

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes: • This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. • This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.	3.3 Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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	3.4.a Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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 should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.											
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.		✓	✓								
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not	3.4.1.a If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
be tied to user accounts.	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).											
	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. Note: If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: Note: This requirement 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.	3.5 Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:											
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	3.5.1 Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	3.5.2.a Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.											
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.											
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for	3.6.a Verify the existence of key-management procedures for keys used for encryption of cardholder data.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store, and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.											
	3.6.c Examine the key-management procedures and perform the following:											
3.6.1 Generation of strong cryptographic keys.	3.6.1 Verify that key-management procedures are implemented to require the generation of strong keys.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.6.2 Secure cryptographic key distribution.	3.6.2 Verify that key-management procedures are implemented to require secure key distribution.											
3.6.3 Secure cryptographic key storage.	3.6.3 Verify that key-management procedures are implemented to require secure key storage.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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).	3.6.4 Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.											
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	3.6.5.a Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
(for example, departure of an employee with knowledge of a clear-text key), 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 purposes.	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.											
	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	3.6.6 Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	3.6.7 Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.											
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	3.6.8 Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: • The Internet • Wireless technologies, • Global System for Mobile communications (GSM) • General Packet Radio Service (GPRS).	4.1 Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:		✓									
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.		✓									
	4.1.b Verify that only trusted keys and/or certificates are accepted.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.		✓									
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)		✓									
	4.1.e For SSL/TLS implementations: Verify that HTTPS appears as a part of the browser Universal Record Locator (URL).• Verify that no cardholder data is required when HTTPS does not appear in the URL.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June 2010.	4.1.1 For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	✓										

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	4.2.a Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.											
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.											
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	✓										

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	5.1.1 For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).	✓										
5.2 Ensure that all anti-virus mechanisms are updated, running, and generate audit logs.	5.2 Verify that all anti-virus software are updated, running, and generate logs by performing the following:											
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.	✓										
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.	✓										

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.	✓										
	5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.	✓										

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize	6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.	✓		✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.	✓		✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Notes: • Risk rankings should be based on industry best practices. For example, criteria for ranking “High” risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as “critical,” and/or a vulnerability affecting a critical system component. • The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.	6.2.a Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as —High.ll)	✓		✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.											
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	6.3.a Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices.											
	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.											
	6.3.d From an examination of written software development processes, and interviews of software developers, verify that:											
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	6.3.1 Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. 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. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	6.3.2.a Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). • Appropriate corrections are implemented prior to release. • Code review results are reviewed and approved by management prior to release.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.											
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	6.4 From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.4.1 Separate development/test and production environments.	6.4.1 The development/test environments are separate from the production environment, with access control in place to enforce the separation.	✓	✓									
6.4.2 Separation of duties between development/test and production environments.	6.4.2 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	✓	✓	✓								
6.4.3 Production data (live PANs) are not used for testing or development.	6.4.3 Production data (live PANs) are not used for testing or development.		✓	✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.4.4 Removal of test data and accounts before production systems become active.	6.4.4 Test data and accounts are removed before a production system becomes active.	✓	✓	✓								
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	6.4.5.a Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.	✓		✓								

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:											
6.4.5.1 Documentation of impact.	6.4.5.1 Verify that documentation of impact is included in the change control documentation for each sampled change.		✓									
6.4.5.2 Documented change approval by authorized parties.	6.4.5.2 Verify that documented approval by authorized parties is present for each sampled change.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	6.4.5.3.a For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.		✓									
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.		✓									
6.4.5.4 Back-out procedures.	6.4.5.4 Verify that back-out procedures are prepared for each sampled change.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.9 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,	6.5.a Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.											
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:											
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	6.5.1 Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.5.2 Buffer overflow.	6.5.2 Buffer overflow (Validate buffer boundaries and truncate input strings.)											
6.5.3 Insecure cryptographic storage.	6.5.3 Insecure cryptographic storage (Prevent cryptographic flaws)											
6.5.4 Insecure communications.	6.54 Insecure communications (Properly encrypt all authenticated and sensitive communications)											
6.5.5 Improper error handling.	6.5.5 Improper error handling (Do not leak information via error messages)											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.5.6 All —Highǁ vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). Note: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.	6.5.6 All —Highǁ vulnerabilities as identified in PCI DSS Requirement 6.2.											
For web applications and application interfaces (internal or external), the following additional requirements apply:												

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
6.5.7 Cross-site scripting (XSS).	6.5.7 Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)											
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).	6.5.8 Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)											
6.5.9 Cross-site request forgery (CSRF).	6.5.9 Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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 • Installing a web-application firewall in front of public-facing web applications	6.6 For public-facing web applications, ensure that either one of the following methods are in place as follows: • Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections • Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.		✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:											
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.	7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
7.1.2 Assignment of privileges is based on individual personnel's job classification and function.	7.1.2 Confirm that privileges are assigned to individuals based on job classification and function (also called —role-based access control‖ or RBAC).	✓	✓	✓	✓							
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	7.1.3 Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.	✓	✓	✓	✓							
7.1.4 Implementation of an automated access control system.	7.1.4 Confirm that access controls are implemented via an automated access control system.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to —deny allll unless specifically allowed. This access control system must include the following:	7.2 Examine system settings and vendor documentation to verify that an access control system is implemented as follows:											
7.2.1 Coverage of all system components.	7.2.1 Confirm that access control systems are in place on all system components.	✓	✓	✓	✓							
7.2.2 Assignment of privileges to individuals based on job classification and function.	7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
7.2.3 Default —deny-allll setting Note: Some access control systems are set by default to “allow-all,” thereby permitting access unless/until a rule is written to specifically deny it.	7.2.3 Confirm that the access control systems have a default — deny-allll setting.	✓	✓	✓	✓							
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	8.1 Verify that all users are assigned a unique ID for access to system components or cardholder data.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.2 In addition to assigning a unique ID, employ 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	8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: • Obtain and examine documentation describing the authentication method(s) used. • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that 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 two-factor authentication.	8.3 To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	8.4.a For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.	✓	✓	✓	✓							
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	8.5 Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.5.1 Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: • Obtain and examine an authorization form for each ID. • Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5.2 Verify user identity before performing password resets.	8.5.2 Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.											
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	8.5.3 Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5.4 Immediately revoke access for any terminated users.	8.5.4 Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.	✓	✓	✓	✓							
8.5.5 Remove/disable inactive user accounts at least every 90 days.	8.5.5 Verify that inactive accounts over 90 days old are either removed or disabled.	✓	✓	✓	✓							
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	8.5.6.a Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.	✓	✓	✓	✓							
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	8.5.7 Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.											
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	8.5.8.a For a sample of system components, examine user ID lists to verify the following: • Generic user IDs and accounts are disabled or removed • Shared user IDs for system administration activities and other critical functions do not exist • Shared and generic user IDs are not used to administer any system components	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	✓	✓	✓	✓							
	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.											
8.5.9 Change user passwords at least every 90 days.	8.5.9.a For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non-consumer users are given guidance as to when, and under what circumstances, passwords must change.	✓	✓	✓	✓							
8.5.10 Require a minimum password length of at least seven characters.	8.5.10.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to meet minimum length requirements.	✓	✓	✓	✓							
8.5.11 Use passwords containing both numeric and alphabetic characters.	8.5.11.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.											
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	8.5.12.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.											
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	8.5.13.a For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.											
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	8.5.14 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
8.5.15 If a session has been idle for more than 15 minutes; require the user to re-authenticate to re-activate the terminal or session.	8.5.15 For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	✓	✓	✓	✓							
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other	8.5.16.a Review database and application configuration settings and verify that all users are authenticated prior to access.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
users. Restrict user direct access or queries to databases to database administrators.	8.5.16.b Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).											
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	8.5.16.d Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. • Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are —lockedǁ to prevent unauthorized use.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.1.1 Use video cameras and/or access control mechanisms 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 the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	9.1.1.a Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.											
	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.											
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized	9.1.2 Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.											
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	9.1.3 Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	9.2.a Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following:• Granting new badges,• Changing access requirements, and• Revoking terminated onsite personnel and expired visitor badges											
	9.2.b Verify that access to the badge system is limited to authorized personnel.											
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.3 Make sure all visitors are handled as follows:	9.3 Verify that visitor controls are in place as follows:											
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	9.3.1 Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.											
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	9.3.2.a Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.											
	9.3.2.b Verify that visitor badges expire.											
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	9.3.3 Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. 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.	9.4.a Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.											
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months											
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a	9.5.a Observe the storage location's physical security to confirm that backup media storage is secure.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
commercial storage facility. Review the location's security at least annually.	9.5.b Verify that the storage location security is reviewed at least annually.											
9.6 Physically secure all media.	9.6 Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).											
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	9.7 Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.7.1 Classify media so the sensitivity of the data can be determined.	9.7.1 Verify that all media is classified so the sensitivity of the data can be determined.											
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	9.7.2 Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.											
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	9.8 Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
9.9 Maintain strict control over the storage and accessibility of media.	9.9 Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.											
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	9.9.1 Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.											
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	9.10 Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:											
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	9.10.1.a Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a —to-be-shredded‖ container has a lock preventing access to its contents.											
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	9.10.2 Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	✓	✓	✓	✓							
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:											
10.2.1 All individual accesses to cardholder data.	10.2.1 Verify all individual access to cardholder data is logged.	✓	✓	✓	✓							
10.2.2 All actions taken by any individual with root or administrative privileges.	10.2.2 Verify actions taken by any individual with root or administrative privileges are logged.	✓	✓	✓	✓							
10.2.3 Access to all audit trails.	10.2.3 Verify access to all audit trails is logged.	✓	✓	✓	✓							
10.2.4 Invalid logical access attempts.	10.2.4 Verify invalid logical access attempts are logged.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.2 5 Use of identification and authentication mechanisms.	10.2.5 Verify use of identification and authentication mechanisms is logged.	✓	✓	✓	✓							
10.2.6 Initialization of the audit logs.	10.2.6 Verify initialization of audit logs is logged.	✓	✓	✓	✓							
10.2.7 Creation and deletion of system-level objects.	10.2.7 Verify creation and deletion of system level objects are logged.	✓	✓	✓	✓							
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation, for each auditable event (from 10.2), perform the following:											
10.3.1 User identification.	10.3.1 Verify user identification is included in log entries.	✓	✓	✓	✓							
10.3.2 Type of event.	10.3.2 Verify type of event is included in log entries.	✓	✓	✓	✓							
10.3.3 Date and time.	10.3.3 Verify date and time stamp is included in log entries.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.3.4 Success or failure indication.	10.3.4 Verify success or failure indication is included in log entries.	✓	✓	✓	✓							
10.3.5 Origination of event.	10.3.5 Verify origination of event is included in log entries.	✓	✓	✓	✓							
10.3.6 Identity or name of affected data, system component, or resource.	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	✓	✓	✓	✓							
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for	10.4.a Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:											
10.4.1 Critical systems have the correct and consistent time.	10.4.1.a Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and that other internal servers receive time only from the central time servers.	✓	✓	✓	✓							
10.4.2 Time data is protected.	10.4.2.a Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	✓	✓	✓	✓							
	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	✓	✓	✓	✓							

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.4.3 Time settings are received from industry-accepted time sources.	10.4.3 Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	✓	✓	✓	✓							
10.5 Secure audit trails so they cannot be altered.	10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Verify that only individuals who have a job-related need can view audit trail files.	✓	✓	✓	✓							
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	✓	✓	✓	✓							
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	10.5.4 Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.	✓	✓	✓	✓							
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).	10.5.5 Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.		✓	✓								

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.	10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.											
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.											
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 back-up).	10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.	✓	✓	✓	✓							
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	11.1.a Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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 any unauthorized devices.	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components • Portable wireless devices connected to system components (for example, by USB, etc.) • Wireless devices attached to a network port or network device											
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.											
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance 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. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have	11.2 Verify that internal and external vulnerability scans are performed as follows:											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
occurred.												
11.2.1 Perform quarterly internal vulnerability scans.	11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.											
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all —Highǁ vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).											
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).	11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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). Scans conducted after network changes may be performed by internal staff.	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).											
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.											
11.2.3 Perform internal and external scans after any significant change. Note: Scans conducted after changes may be	11.2.3.a Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
performed by internal staff.	11.2.3.b Review scan reports and verify that the scan process includes rescans until: · For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS • For internal scans, a passing result is obtained or all —Highǁ vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.											
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
11.3 Perform external and internal penetration testing at least once a year 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). These penetration tests must include the following:	11.3.a Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.											
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.											
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
11.3.1 Network-layer penetration tests	11.3.1 Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.											
11.3.2 Application-layer penetration tests	11.3.2 Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to 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. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	11.4.a Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.											
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.											
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For file-integrity monitoring 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. File-integrity	11.5.a Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files			✓								

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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 merchant or service provider).	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.			✓								
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).											
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	12.1.2.a Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.											
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.											
12.1.3 Includes a review at least annually and updates when the environment changes.	12.1.3 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	12.2 Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.	✓	✓	✓	✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	12.3 Obtain and examine the usage policies for critical technologies and perform the following:											
12.3.1 Explicit approval by authorized parties	12.3.1 Verify that the usage policies require explicit approval from authorized parties to use the technologies.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.3.2 Authentication for use of the technology	12.3.2 Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).											
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices.											
12.3.4 Labeling of devices to determine owner, contact information and purpose	12.3.4 Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.											
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies require acceptable uses for the technology.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies require acceptable network locations for the technology.											
12.3.7 List of company-approved products	12.3.7 Verify that the usage policies require a list of company-approved products.											
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	12.3.8 Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.											
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	12.3.9 Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	12.3.10.a Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.											
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.											
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	12.4 Verify that information security policies clearly define information security responsibilities for all personnel.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.5 Assign to an individual or team the following information security management responsibilities:	12.5 Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:											
12.5.1 Establish, document, and distribute security policies and procedures.	12.5.1 Verify that responsibility for creating and distributing security policies and procedures is formally assigned.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.											
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	12.5.3 Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.											
12.5.4 Administer user accounts, including additions, deletions, and modifications	12.5.4 Verify that responsibility for administering user account and authentication management is formally assigned.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.5.5 Monitor and control all access to data.	12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.											
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	12.6.a Verify the existence of a formal security awareness program for all personnel.											
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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.	12.6.1. a Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).											
	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.											
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	12.6.2 Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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.	12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	12.8 If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:											
12.8.1 Maintain a list of service providers.	12.8.1 Verify that a list of service providers is maintained.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
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.	12.8.2 Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.											
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	12.8.3 Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.											
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	12.8.4 Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.9 Obtain and examine the Incident Response Plan and related procedures and perform the following:											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.9.1 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 back-up processes • 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	12.9.1.a Verify that the Incident Response Plan includes: Roles, responsibilities, and communication 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 back-up processes • Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) • Coverage and responses for all critical system components • Reference or inclusion of incident response procedures from the											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	payment brands											
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.											
12.9.2 Test the plan at least annually.	12.9.2 Verify that the plan is tested at least annually.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	12.9.3 Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.											
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	12.9.4 Verify through observation and review of policies that staff with responsibility for security-breach response is periodically trained.											

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	12.9.5 Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.											
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	12.9.6 Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: 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.	A.1 Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.											

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

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	A.1.1 If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID. • All CGI scripts used by an entity must be created and run as the entity's unique user ID.	✓			✓							
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	A.1.2.a Verify the user ID of any application process is not a privileged user (root/admin).	✓			✓							

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). Important: An entity's files may not be shared by group.	✓										
	A.1.2.c Verify that an entity's users do not have write access to shared system binaries.	✓		✓								
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.	✓	✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU	✓	✓									

PCI REQUIREMENT	PCITESTING PROCEDURES	PARTNER SOLUTIONS PLEASE REFER TO THE RESPECTIVE PARTNER PCI SOLUTION GUIDE FOR APPLICABILITY MAPPING										
		VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	1. HARDWARE	2. AUTHENTICATION	3. LOGGING, MONITORING	4. ENDPOINT SECURITY	5. ENCRYPTION	6. AVAILABILITY	7. OTHER
Number of PCI DSS Controls Addressed		104	116	113	80							
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	A.1.3 Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	✓	✓	✓	✓							
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	A.1.4 Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.											

Acknowledgements:

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading PCI QSA firm, provided PCI guidance and control interpretation aligned to PCI DSS v. 2.0 and the Reference Architecture described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire®

Coalfire Systems is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire® has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C., and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire® has developed a new generation of cloud-based IT GRC tools under the Navis™ brand that clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA. For more information, visit www.coalfire.com.

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