vmware PARTNER NETWORK

Solution Guide for Payment Card Industry (PCI)

Partner Addendum

LogRhythm™ vmware®

LogRhythm Addendum to VMware Solution Guide for Payment Card Industry Data Security Standard

The findings and recommendations contained in this document are provided by VMware-certified professionals at Coalfire®, a leading PCI Qualified Security Assessor and independent IT audit firm. Coalfire's results are based on detailed document inspections and interviews with the vendor's technical teams. Coalfire's guidance and recommendations are consistent with PCI DSS control intent generally accepted by the QSA assessor community. The results contained herein are intended to support product selection and high-level compliance planning for VMware-based cloud deployments. More information about Coalfire can be found at www.coalfire.com.

If you require more information specific to this solution guide, you may contact us here: www.coalfire.com/logrhythm

Coalfire®
IT Governance, Risk & Compliance

Table of Contents

1. Introduction

Merchants and service providers that transmit, store or process payment card information are required to meet all PCI DSS controls in order to fulfill the compliance standard for accepting payment cards. LogRhythm is working with VMware to provide solutions that help customers achieve PCI compliance through log and event management in virtual, physical and hybrid environments.

Clear visibility into all aspects of an organization's IT systems and user activity, whether that of employees, partners or customers, is imperative in today's networked environments. IT administrators and security professionals are tasked with monitoring and protecting an overwhelming number of transactions and events that traverse their systems every day.

Having an effective log and event management solution to gain network visibility and better understand the overall health of a networked environment is not only a valued asset for IT professionals, it has become a requirement for regulatory compliance. When deploying a log and event management solution for compliance, organizations should ensure that the information provided by event logging systems is meaningful and relevant and that its collection is consistent and assured. This requires assuring that specific types of data are logged with a secure chain of custody so that an effective audit trail can be constructed.

LogRhythm delivers out-of-the-box packages for PCI compliance, either directly meeting or augmenting 80 individual PCI mandates. This includes fully integrated File Integrity Monitoring that directly meets PCI DSS 11.5 – without requiring an additional third-party platform. PCI compliance is helped by fully automated packages that include out-of-the-box reports, investigations, alarms and layouts, directly mapped and clearly labeled to correspond to each supported mandate. LogRhythm also has out-of-the-box support for point-of-sale systems, with advanced agent technology that enables collecting from remote retail locations. Agents are centrally deployed and managed and can encrypt and compress data for secure collection without negatively impacting bandwidth. If a connection is lost, the agent will continue to collect data at the remote location until communication is restored, to ensure that no data is lost.

LogRhythm and VMware provide a framework that includes both LogRhythm and VMware systems, as well as other partner products, that enables customers to meet their PCI DSS control requirements. The appropriate integration with infrastructure products provides customers with additional capabilities for successfully navigating the compliance landscape. LogRhythm is architected to monitor components within a PCI environment, whether fully virtualized or leveraging a hybrid infrastructure of virtual and physical components, to detect and prevent confidential data leakage within the PCI path. This includes auditing user information and resource access, as well as independently monitoring virtual and/or physical host activity and communication between internal and external components, including shared virtual resources.

This paper examines the capabilities of the LogRhythm SIEM 2.0 platform in achieving Payment Card Industry (PCI) Data Security Standard (DSS) compliance, and describes how this solution aligns to PCI DSS controls.

VMware

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 the VMware Solution Guide for PCI. 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

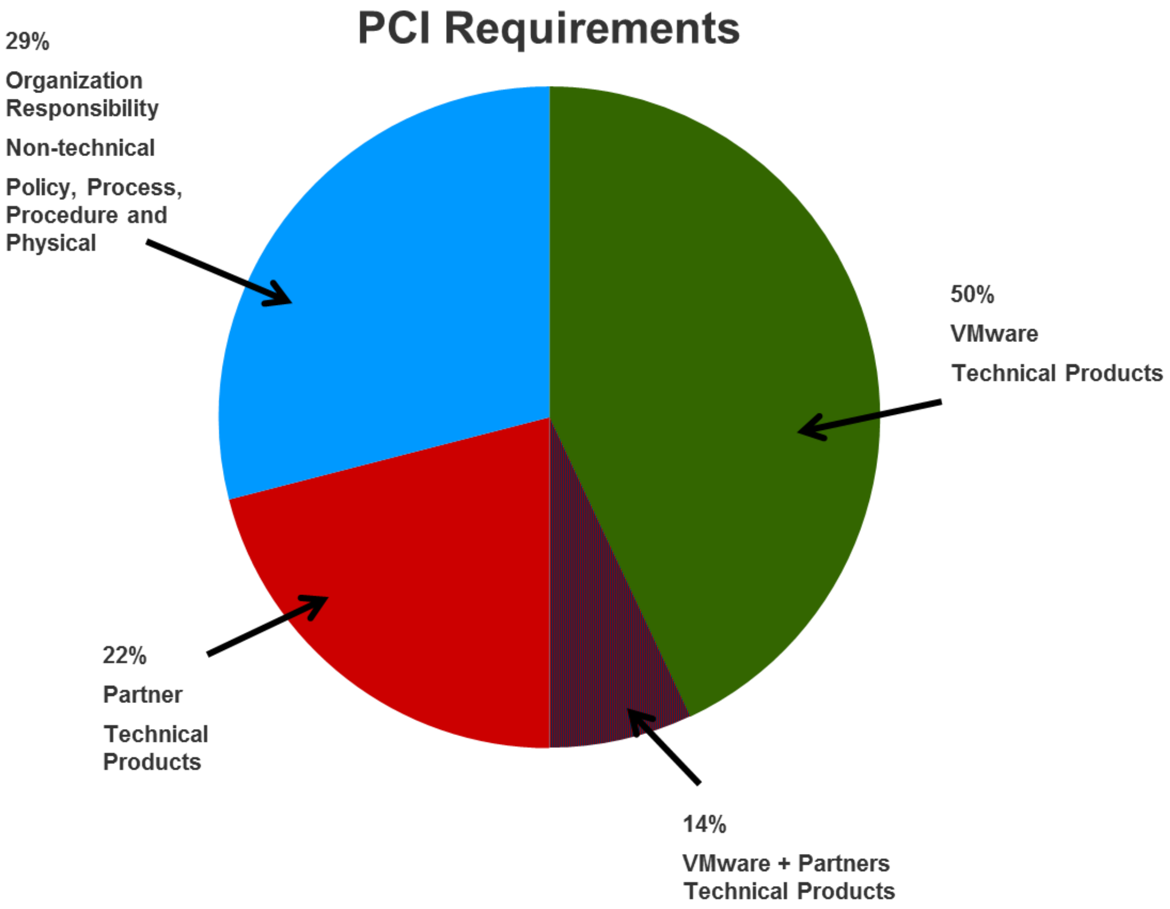


Figure 2: VMware + LogRhythm Product Capabilities for a Trusted Cloud

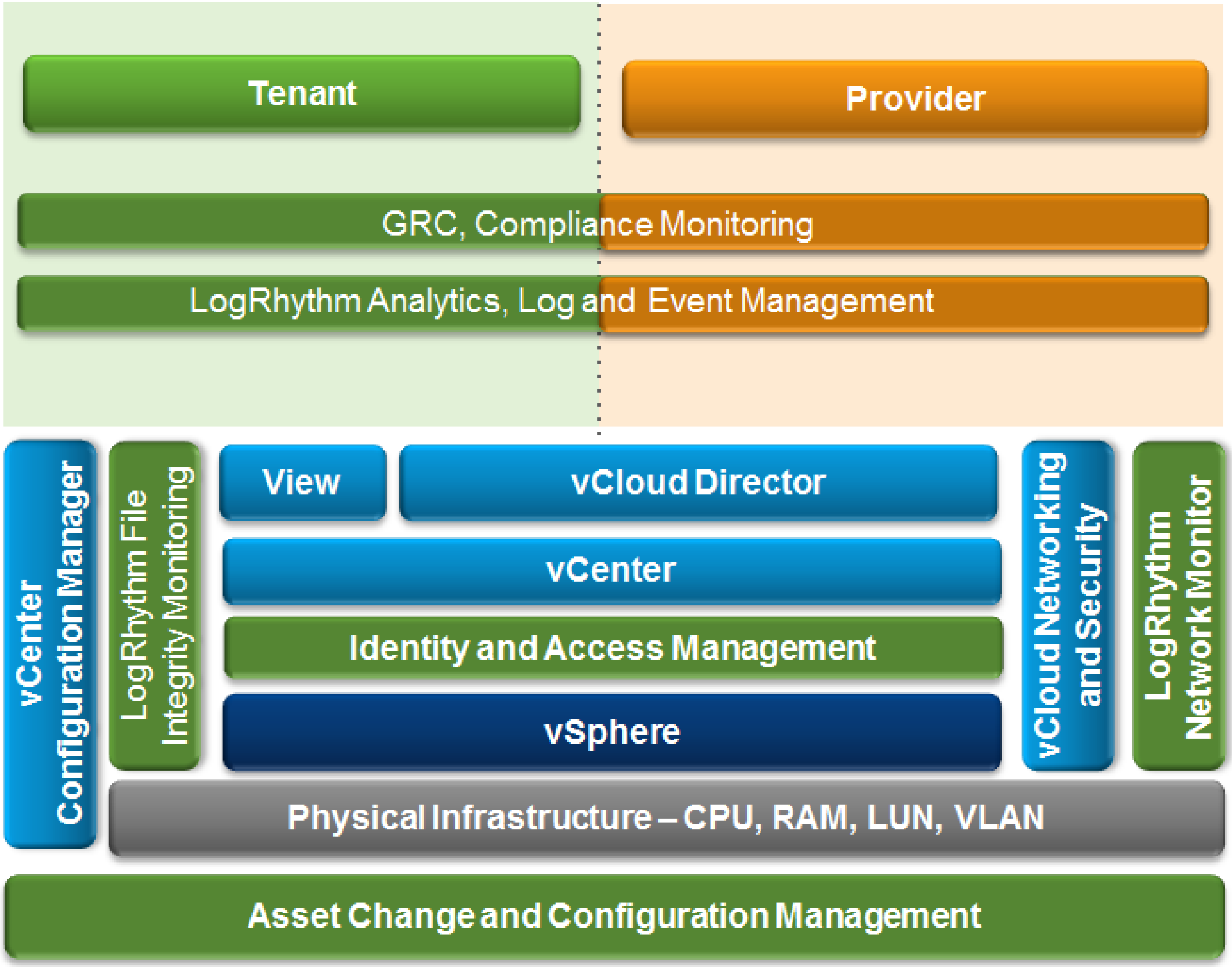
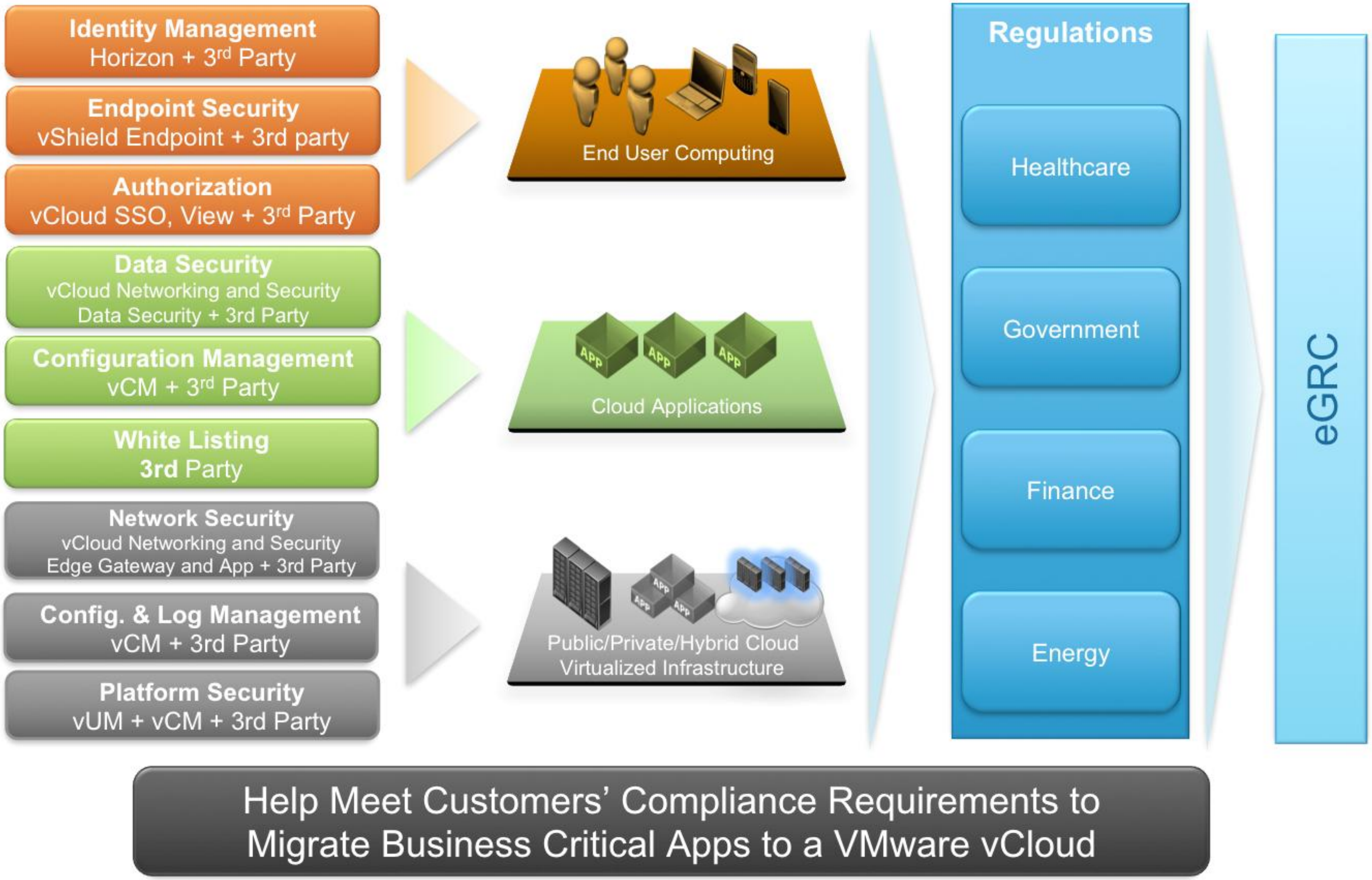

Tenant
Provider
GRC, Compliance Monitoring
LogRhythm Analytics, Log and Event Management
vCenter Configuration Manager
LogRhythm File Integrity Monitoring
View
vCloud Director
vCenter
Identity and Access Management
vSphere
vCloud Networking and Security
LogRhythm Network Monitor
Physical Infrastructure – CPU, RAM, LUN, VLAN
Asset Change and Configuration Management

Figure 3: Help Meet Customers' Compliance Requirements to Migrate Business Critical Apps to a VMware vCloud


Identity Management
Horizon + 3rd Party
Endpoint Security
vShield Endpoint + 3rd party
Authorization
vCloud SSO, View + 3rd Party
Data Security
vCloud Networking and Security
Data Security + 3rd Party
Configuration Management
vCM + 3rd Party
White Listing
3rd Party
Network Security
vCloud Networking and Security
Edge Gateway and App + 3rd Party
Config. & Log Management
vCM + 3rd Party
Platform Security
vUM + vCM + 3rd Party
End User Computing
App
Cloud Applications
Public/Private/Hybrid Cloud
Virtualized Infrastructure
Regulations
Healthcare
Government
Finance
Energy
eGRC
Help Meet Customers' Compliance Requirements to
Migrate Business Critical Apps to a VMware vCloud

2. 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."

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

For additional information on VMware compliance solutions for PCI, please refer to the
http://www.vmware.com/solutions/datacenter/cloud-security-compliance/protect-critical-applications.html

Figure 4: LogRhythm Solution

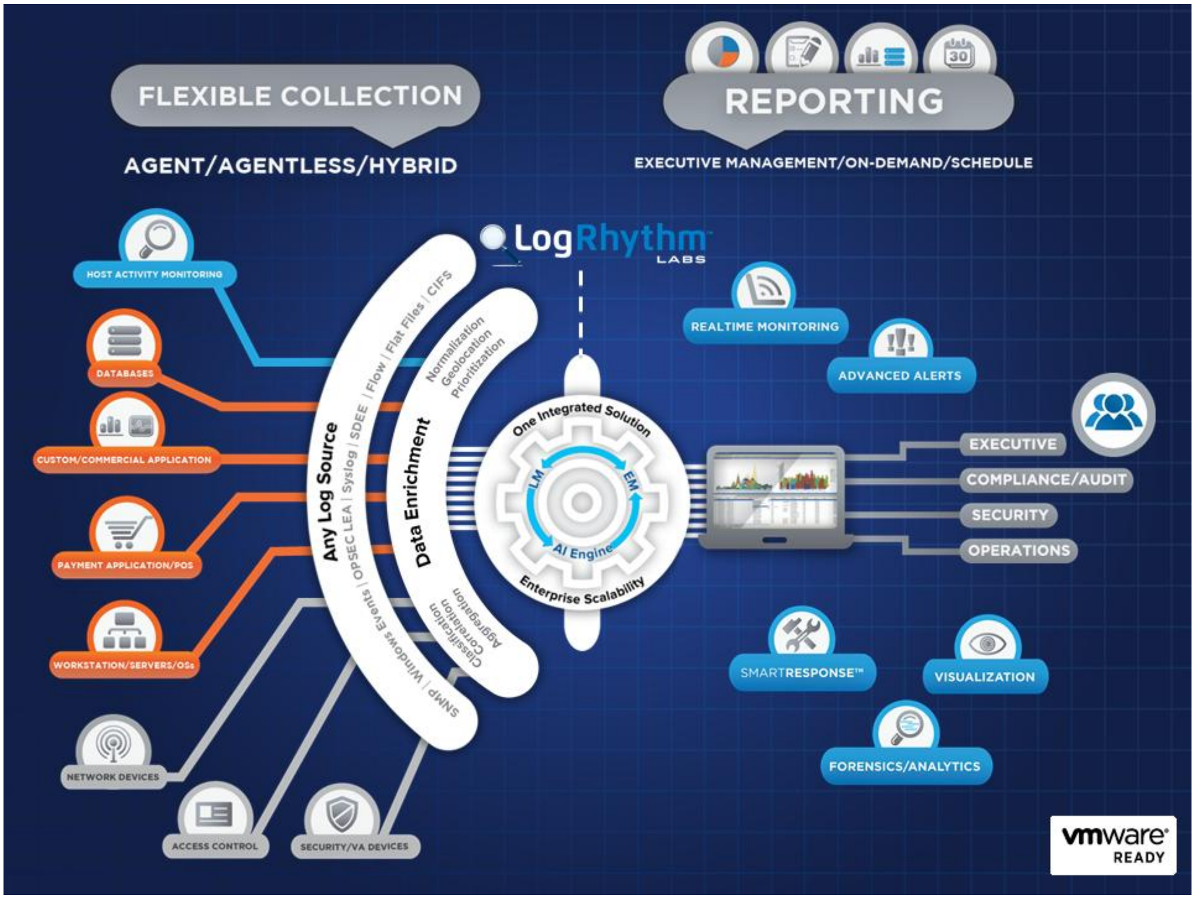


Figure 5: VMware Cloud Computing Partner Integration

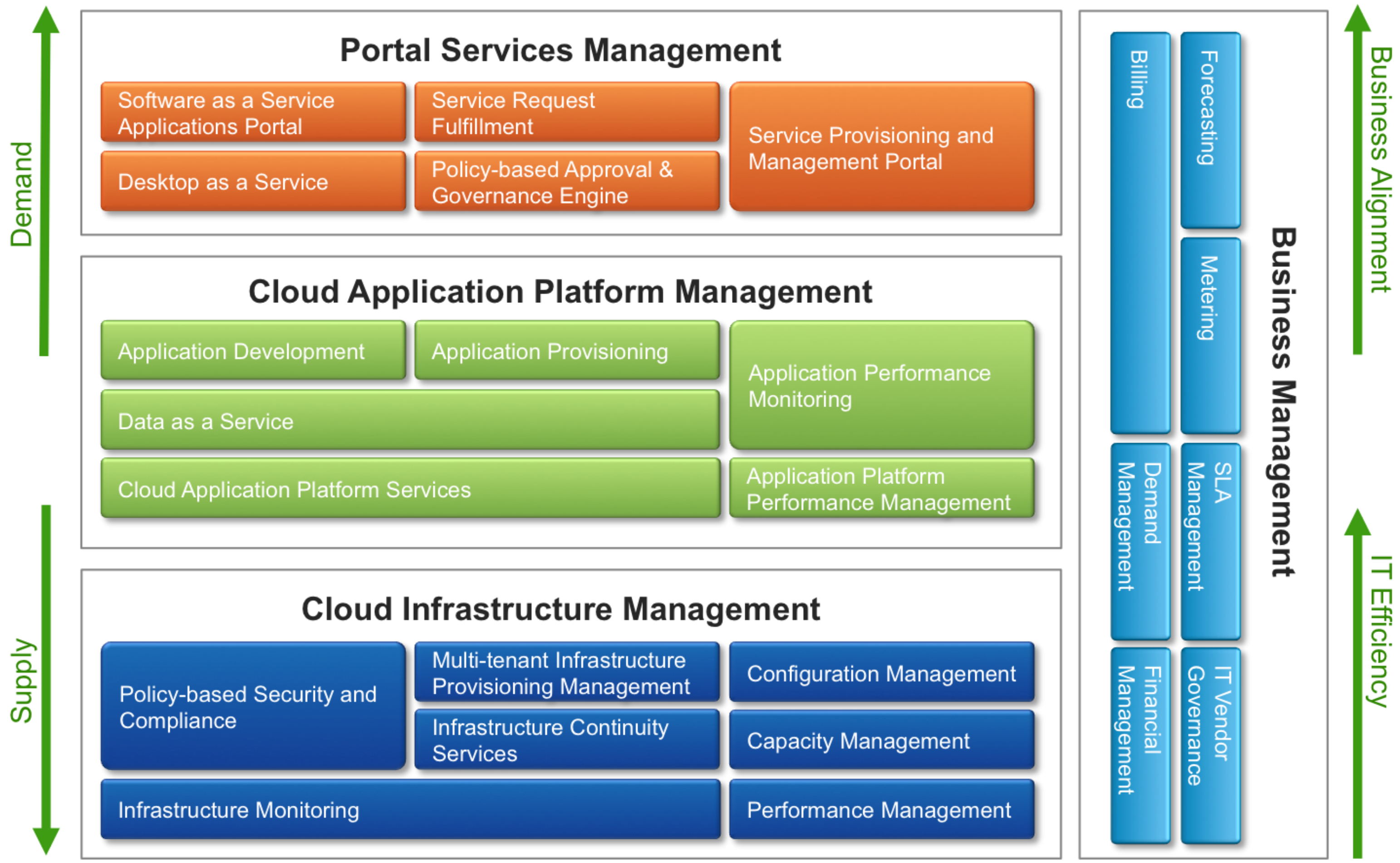
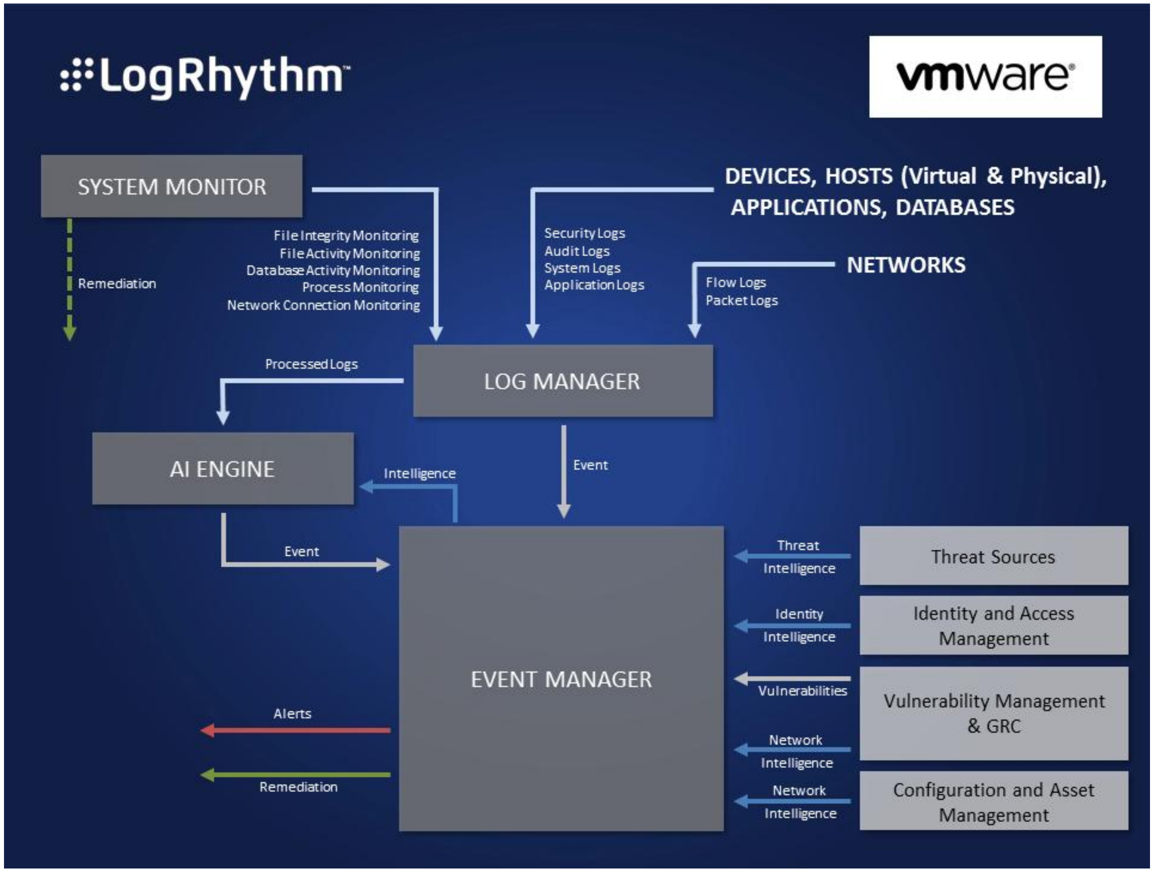

Demand
Supply
Portal Services Management
Software as a Service Applications Portal
Service Request Fulfillment
Service Provisioning and Management Portal
Desktop as a Service
Policy-based Approval & Governance Engine
Cloud Application Platform Management
Application Development
Application Provisioning
Application Performance Monitoring
Data as a Service
Cloud Application Platform Services
Application Platform Performance Management
Cloud Infrastructure Management
Policy-based Security and Compliance
Multi-tenant Infrastructure Provisioning Management
Configuration Management
Infrastructure Continuity Services
Capacity Management
Infrastructure Monitoring
Performance Management
Business Management
Billing
Forecasting
Metering
Demand Management
SLA Management
Financial Management
IT Vendor Governance
Business Alignment
IT Efficiency

Figure 6: LogRhythm and VMware Integration

Achieving PCI compliance is not a simple task. It is difficult for many organizations to navigate the current landscape of information systems and adequately fulfill all PCI DSS requirements. LogRhythm, working with VMware, is continuing its leadership role in the industry by providing file integrity monitoring and log and event management systems from the data center to the cloud, to help clients meet their compliance needs.

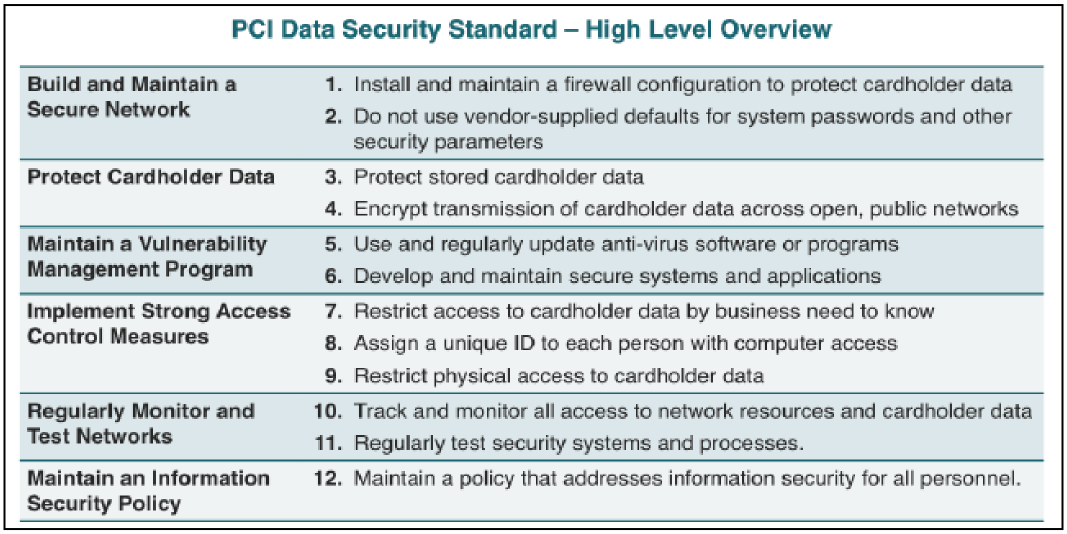


3. Overview of PCI as it applies to Cloud/Virtual Environments

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

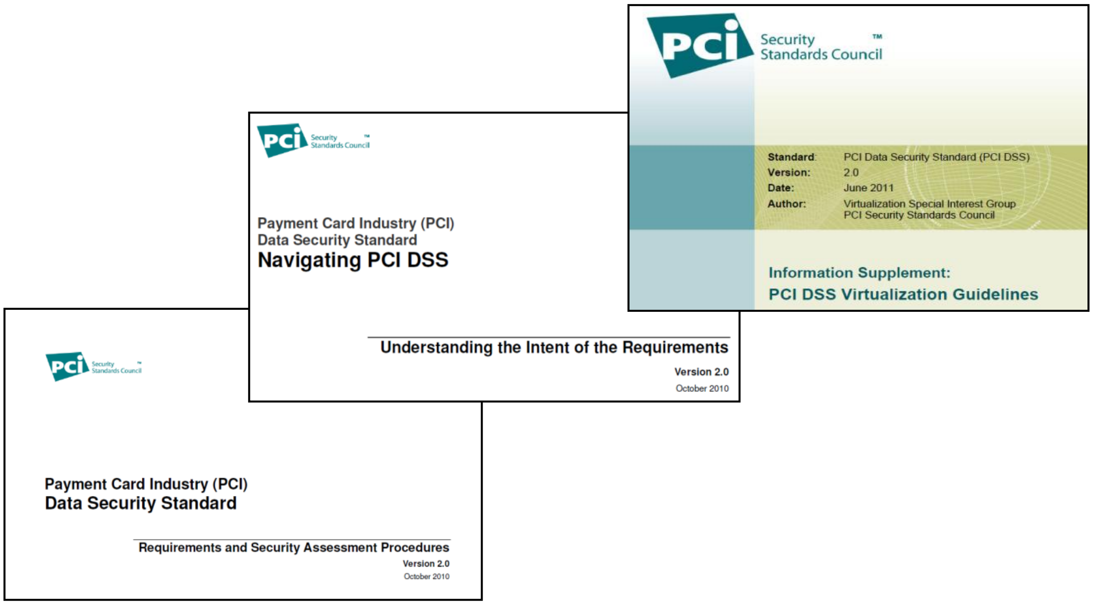


PCI Data Security Standard – High Level Overview

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).

Figure 7: Navigating PCI DSS



PCI Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: June 2011
Author: Virtualization Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS Virtualization Guidelines

PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard
Navigating PCI DSS

Understanding the Intent of the Requirements
Version 2.0
October 2010

PCI Security Standards Council

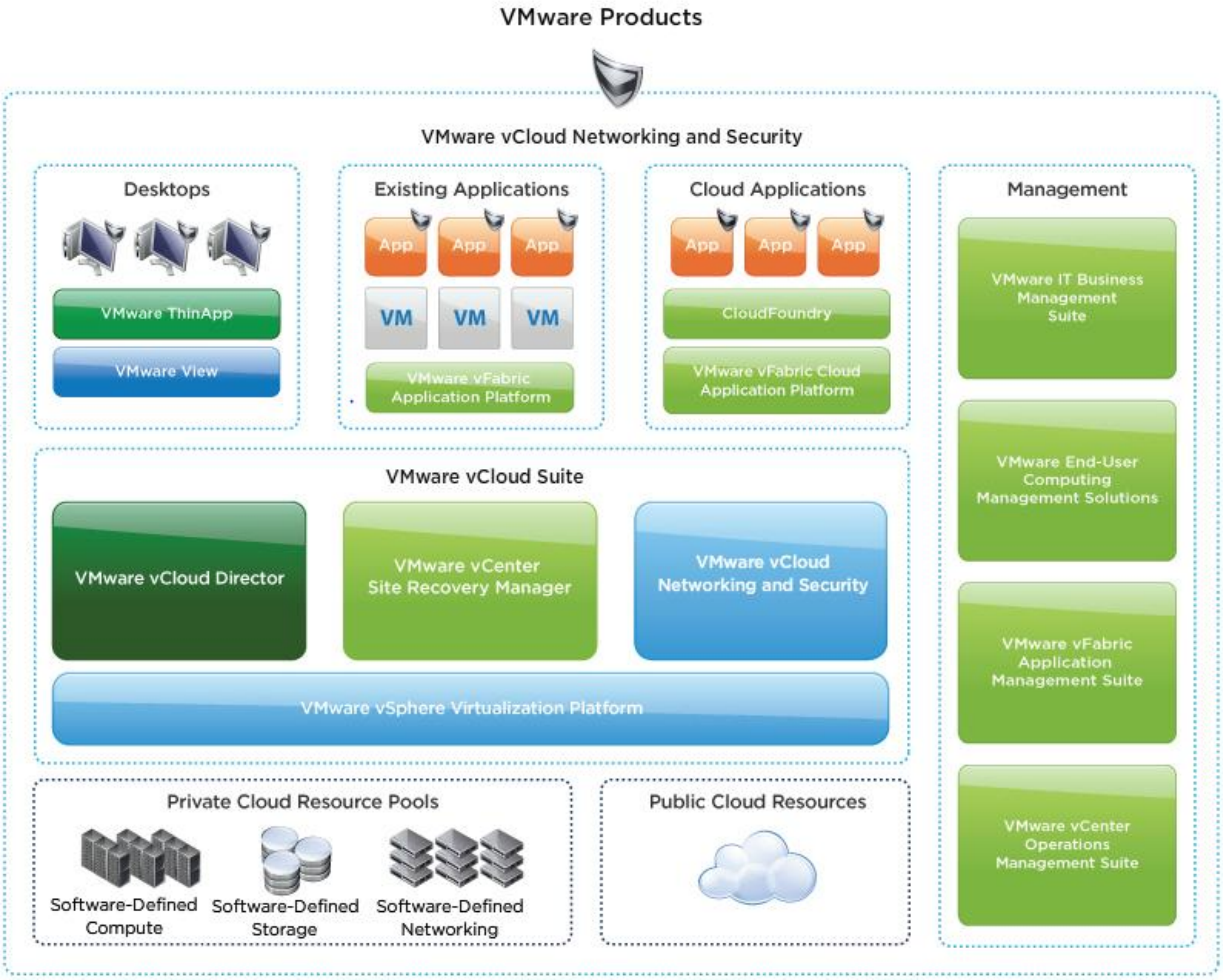
Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 2.0
October 2010

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.

Figure 8: VMware PCI Compliance Products


VMware Products
VMware vCloud Networking and Security
Desktops
VMware ThinApp
VMware View
Existing Applications
App
App
App
VM
VM
VM
VMware vFabric Application Platform
Cloud Applications
App
App
App
CloudFoundry
VMware vFabric Cloud Application Platform
Management
VMware IT Business Management Suite
VMware End-User Computing Management Solutions
VMware vFabric Application Management Suite
VMware vCenter Operations Management Suite
VMware vCloud Suite
VMware vCloud Director
VMware vCenter Site Recovery Manager
VMware vCloud Networking and Security
VMware vSphere Virtualization Platform
Private Cloud Resource Pools
Software-Defined Compute
Software-Defined Storage
Software-Defined Networking
Public Cloud Resources

4. LogRhythm PCI Compliance Solution

Table 2: LogRhythm Solutions

LOGRHYTHM PCI COMPLIANCE SOLUTION	**LogRhythm Log Management and SIEM** LogRhythm is an enterprise-class platform that combines Log Management & SIEM 2.0, File Integrity Monitoring, and Host Activity Monitoring into a single integrated solution. It is designed to address an ever-changing landscape of threats and challenges, with a full suite of high-performance tools for security, compliance, and operations. LogRhythm's SIEM 2.0 platform delivers: • Fully Integrated Log & Event Management • Advanced Correlation and Pattern Recognition • Extended Visibility and Context ○ Independent Host Activity Monitoring ○ File Activity Monitoring ○ Enterprise-wide Network Visibility • Powerful, Rapid Forensics • Intelligent, Process-Driven Smart**Response**™ • Ease-of-use and Simplified Management Valuable information can be derived from log data – originating from applications, databases, servers, network devices or host systems. LogRhythm enables organizations to detect and respond to advanced threats, automate compliance assurance and intelligently optimize IT operations by automating the collection, organization, analysis, archiving and reporting of all log data. By integrating Log Management & SIEM 2.0, with File Integrity Monitoring and Host Activity Monitoring in one solution LogRhythm helps customers: • Expand and accelerate threat detection & response capabilities • Reduce acquisition costs and management overhead • Automate compliance • Increase ROI It is operated and managed through a wizard-driven console. With LogRhythm, enterprises can invest in a single solution to address security, compliance, and operations issues related to requirements and challenges throughout their IT organizations. **Integrated File Integrity Monitoring** With the addition of File Integrity Monitoring, LogRhythm can be used to monitor for and alert on a variety of malicious behaviors, from improper user access of confidential files to botnet related breaches and transmittal of sensitive data. The combined solution allows organizations to meet specific regulatory compliance requirements, such as Payment Card Industry Data Security Standard (PCI DSS) 11.5 and 12.9, without purchasing a separate product.

5. LogRhythm PCI Requirements Matrix (Overview)

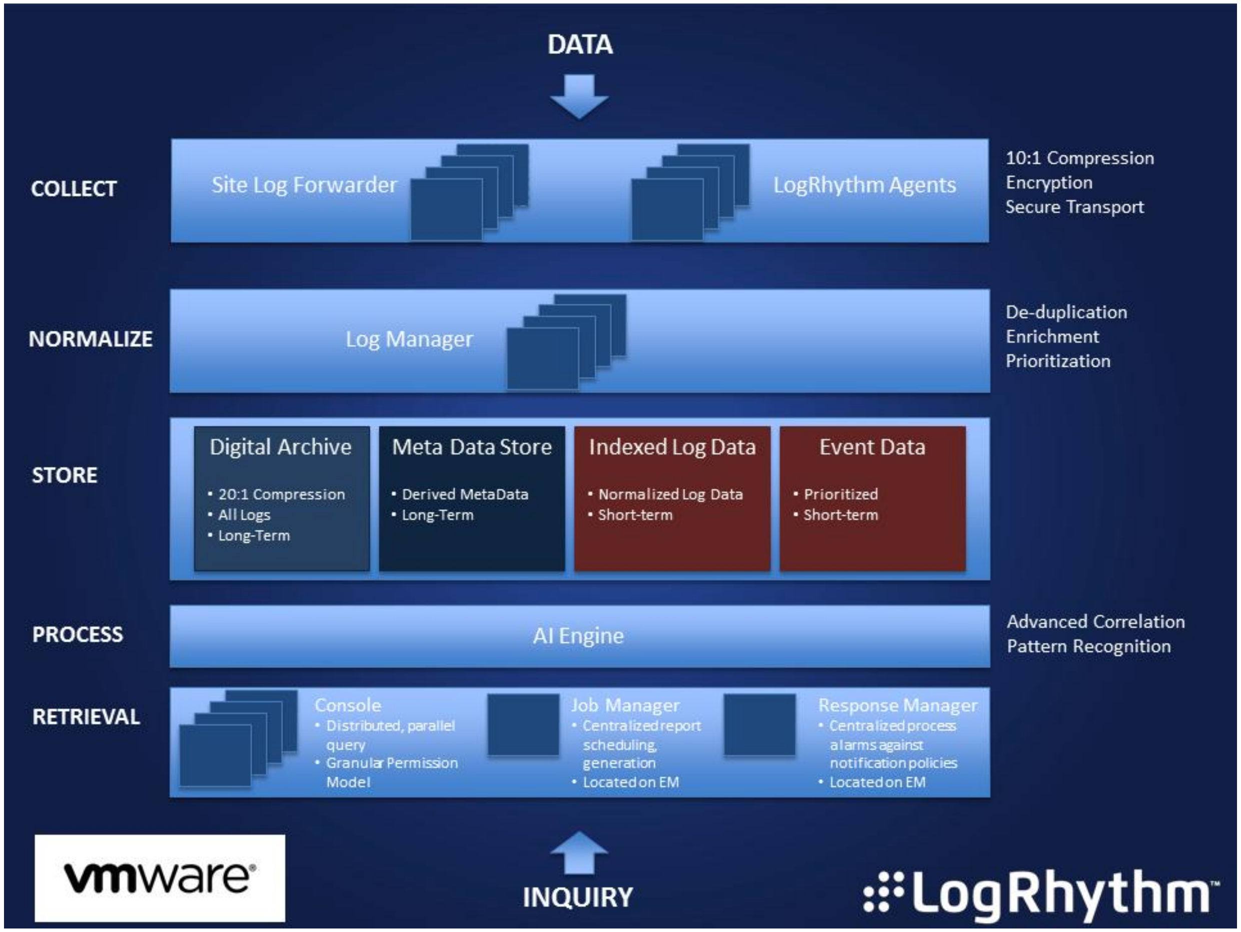
LogRhythm's PCI DSS Compliance Package includes extensive log collection support. When properly deployed and configured the LogRhythm solution either fully meets or augments the following PCI DSS requirements:

Table 3: PCI DSS Requirements Matrix

PCI DSS 2.0 REQUIREMENT	NUMBER OF PCI REQUIREMENTS	NUMBER OF CONTROLS MET OR AUGMENTED BY LOGRHYTHM	COLLECTIVE TOTAL CONTROLS ADDRESSED BY LOGRHYTHM
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	25	12	12
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	24	4	4
Requirement 3: Protect stored cardholder data	33	1	1
Requirement 4: Encrypt transmission of cardholder data across open, public networks	9	1	1
Requirement 5: Use and regularly update anti-virus software or programs	6	4	4
Requirement 6: Develop and maintain secure systems and applications	32	14	14
Requirement 7: Restrict access to cardholder data by business need to know	7	2	2
Requirement 8: Assign a unique ID to each person with computer access	32	11	11
Requirement 9: Restrict physical access to cardholder data	28	2	2
Requirement 10: Track and monitor all access to network resources and cardholder data	29	22	22
Requirement 11: Regularly test security systems and processes.	24	4	4
Requirement 12: Maintain a policy that addresses the information security for all personnel	40	3	3
TOTAL	**297**	**80**	**80**
Note: Control totals do not add up to 297 due to overlapping features of LogRhythm products.			

Figure 9: Diagrammatic Representation of LogRhythm PCI Suite

LogRhythm’s SIEM 2.0 platform with integrated file integrity monitoring provides a solution that customers can adapt quickly to their VMware environments.



PCI Cloud Compliance Solution Details

The following matrix maps the PCI DSS controls to the functionality of the LogRhythm PCI Cloud Compliance Solution. LogRhythm is an enterprise-class platform that seamlessly combines Log Management & SIEM 2.0, File Integrity Monitoring, and Host Activity Monitoring into a single integrated solution. It is designed to address an ever-changing landscape of threats and challenges, with a full suite of high-performance tools for security, compliance, and operations. LogRhythm delivers comprehensive, useful and actionable insight into what is really going on in and around an enterprise IT environment.

LogRhythm provides solutions to support or meet PCI DSS controls. Additional policy, process or technologies may be needed to be used in conjunction with LogRhythm's solutions to fully comply with PCI DSS controls.

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
1. Install and Maintain a firewall configuration to protect data	1.1.1, 1.1.5a, 1.1.5.b, 1.1.6.b, 1.2.1.a, 1.2.1.b, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.5, 1.4.a	LogRhythm meets or augments the following specific controls: • LogRhythm directly supports testing procedure 1.1.1 by providing details of firewall and router configuration or policy changes via investigations, reports, and tails. Testing for a formal process is still required. • LogRhythm directly supports testing procedure 1.1.5.a by providing details of allowed or denied, secure or insecure network protocols and ports within the organizational network infrastructure via investigations, reports, and tails. Verification is required of documented business need. • LogRhythm supports testing procedure 1.1.6.b by providing details of allowed or denied network protocols and ports within the organizational network infrastructure. • LogRhythm augments the testing process for 1.2.1.a and 1.2.1.b by providing details of allowed or denied inbound or outbound network traffic to the cardholder data environment via investigations, reports, and tails. This will allow for verification that inbound and outbound traffic is being restricted or allowed.

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		• LogRhythm augments the testing process for 1.2.2 by providing alarms on firewall synchronization critical or error conditions and also by providing details of firewall synchronization conditions via investigations and reports. • LogRhythm augments the testing process for procedure 1.3.1 by providing details of allowed or denied network protocols or ports between the DMZ environment and the organization’s internal network environment via investigations, reports, and tails. • LogRhythm augments the testing process for 1.3.2 by being able to detect and alert on allowed or denied network traffic between the external Internet and the organizations internal network environment via investigations, reports, and tails • LogRhythm augments the testing process for 1.3.3 by providing details of allowed or denied network traffic that is inbound or outbound between the external Internet and cardholder data environment via investigations, reports, and tails. • LogRhythm augments the testing process for 1.3.5 by providing details of allowed or denied network traffic outbound from the cardholder data environment to the external Internet via investigations, reports, and tails. • LogRhythm provides AIE rules, alarms, investigations, and reports to support PCI DSS control requirement 1.4.a. • LogRhythm augments the testing process for procedure 1.4.a by providing alarms on host firewall critical or error conditions and also by providing details of host firewall conditions via investigations and reports.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.2.2.a, 2.2.2.b, 2.3.b	LogRhythm meets or augments the following specific controls: • LogRhythm provides AIE rules, investigations, and reports to support PCI-DSS control requirement 2.1. LogRhythm directly supports testing procedure

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		2.1 by providing AIE rule alarms and details of known vendor default account authentication failures or successes via investigations and reports. • LogRhythm provides host activity monitoring that monitors running processes and services in support of 2.2.2.a and 2.2.2.b. Verification that only necessary services are enabled and justification for insecure services is still required. • LogRhythm augments the testing process for procedure 2.3.b by providing details of insecure network protocols or ports that are allowed or denied within the organizational network infrastructure and insecure processes are starting or stopping via investigations, reports, and tails.
3. Protect stored cardholder data	3.6.7	LogRhythm meets or augments the following specific controls: • LogRhythm augments the testing process for 3.6.7 by providing details of key integrity activity via investigations, reports, and tails on LogRhythm's File Integrity Monitor Agent. LogRhythm's File Integrity Monitor can be configured to monitor key file or directory activity, deletions, modification, and permission changes. The file integrity capability is completely automated, the agent can be configured to either scan for files/directory changes on a schedule or the kernel level driver can automatically detect file integrity activity in real-time.
4. Encrypt transmission of cardholder data across open, public networks	4.1	LogRhythm meets or augments the following specific controls: • LogRhythm augments the testing process for 4.1 by providing details of insecure network protocols or ports that are allowed or denied within the organizational network infrastructure and insecure processes that are starting or stopping via investigations, reports, and tails. LogRhythm is capable of alarming on conditions where a system observes unencrypted information passed when encrypted traffic is expected.

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
5. Use and regularly update anti-virus software or programs	5.1, 5.2.b, 5.2.c, 5.2.d	LogRhythm meets or augments the following specific controls: • LogRhythm supports testing for 5.1 by verifying that the service is running on the systems commonly affected malware and detecting or alerting on changes to the service. • LogRhythm supports testing for 5.2.b by providing alarms on antivirus critical or error conditions and also provides detailed information on malware and antivirus detection via investigations and reports. Detection for when new signatures are installed is also supported. • LogRhythm augments testing procedure 5.2.c by providing visibility to antivirus signature updates and scanning activities, successes and failures via alarms, investigations, and reports • LogRhythm's centralized log collection, management, and archival functionality directly supports PCI-DSS control requirement 5.2.d by automating the process of collecting and retaining the antivirus software audit trails. LogRhythm creates archive files of all collected antivirus log entries which are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on retention policy.
6. Develop and maintain secure systems and applications	6.1.a, 6.1.b, 6.3.a, 6.4.1, 6.4.2, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.7, 6.5.8, 6.5.9, 6.6	LogRhythm meets or augments the following specific controls: • LogRhythm directly supports testing procedure 6.1.a by providing alarms on software update critical or error conditions and also by providing details on software update conditions via investigations and reports. LogRhythm is able to support 6.1.b by running reports and showing that specific patches are deployed within one month. • LogRhythm augments the testing process for 6.3.a by providing an intelligence system for logs to be sent to rules that can be created to provide proper alarming, reporting, and enhancement to the abilities of any

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		custom application to be used in the cardholder data environment. • LogRhythm augments the testing process for procedure 6.4.1 by providing details on allowed or denied network protocols or ports between the test network environment and all other internal production network environments via investigations, reports, and tails. • LogRhythm augments the testing process for 6.4.2 by providing details on allowed or denied network traffic between the test network environment and all other internal network environments via investigations, reports, and tails. • LogRhythm augments the testing process for 6.5 by providing alarms and investigation details on detected vulnerabilities. • LogRhythm augments the testing process for 6.6 by providing alarms and investigation details on detected vulnerabilities. LogRhythm can address either solution by working in conjunction with web exploit systems, such as Intrusion Detection Systems, Web-Application Firewalls, Stateful Inspection Firewalls, Web Servers, and other log sources to analyze detected potential abuses as well as provide a way to investigate suspected breaches.
7. Restrict access to cardholder data by business need to know	7.1.1, 7.1.2	LogRhythm meets or augments the following specific controls: • LogRhythm augments the testing process for 7.1.1 and 7.1.2 by providing details on privileged access, host authentication, application access via investigations and reports. Access to cardholder data can be monitored by the custodian(s) of the data in real-time by collecting access control system data. Account creation, privilege assignment and revocation, and object access can be validated using LogRhythm.
8. Assign a unique ID to each person with computer access	8.1, 8.5.1, 8.5.4, 8.5.5, 8.5.6.a, 8.5.6.b, 8.5.8.a, 8.5.9.a, 8.5.13.a, 8.5.14.a, 8.5.16.a	LogRhythm meets or augments the following specific controls: • LogRhythm augments the testing process for procedure 8.1 by providing

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		details on account management activity such as account creation, account deletion, and account modification via reports. Account creation can be monitored through reporting and investigations of logs pertaining to the creation and modification of accounts. • LogRhythm augments the testing process for procedure 8.5 by providing alarms on database account access granting or revocation and details on account management, account granting or revocation, and authentication activity via investigations and reports. LogRhythm also provides details on vendor account management and authentication activity via investigations and reports.
9. Restrict physical access to cardholder data	9.1, 9.1.1.c	LogRhythm meets or augments the following specific controls: • LogRhythm provides AIE rules, alarms, investigations, and reports to support PCI-DSS control requirement 9.1. LogRhythm augments the testing process for procedures 9.1 and 9.1.1.c by providing alarms for physical access failures and details on other physical access activity via investigations and reports.
10. Track and monitor all access to network resources and cardholder data	10.2, 10.2.1, 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, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6.a, 10.7.a	LogRhythm meets or augments the following specific controls: • LogRhythm directly supports testing procedure 10.2 by providing the core function of centralized log collection, management, and archival. LogRhythm provides alarms on authentication failures from default, disabled, terminated, privileged accounts, object disposal failures and audit log initializations. LogRhythm provides details of user access failures or successes to audit log files, cardholder data files, system-level objects, and applications via investigations and reports. LogRhythm provides details of privileged account management such as creation, deletion, modification, authentication failures and successes, granting or revoking of access, privilege escalation and failures or successes to access files, objects, and applications via investigations and reports. LogRhythm also provides details

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		on the creation and deletion of system level objects and audit log initializations via investigations and reports • LogRhythm directly supports testing procedure 10.3 by parsing account and login information, assigning each log event a specific classification type, specifying a centralized time stamp, extracting success or failure information, identifying the host, IP, application, login originating each event, identifying affected data, components, resources and other details useful for forensic investigation of the audit logs. • LogRhythm directly supports testing procedure 10.3.3 by independently synchronizing the timestamps of all collected log entries, ensuring that all log data is time-stamped to a standard time regardless of the time zone and clock settings of the log source. • LogRhythm directly supports testing procedure 10.4 by independently synchronizes the timestamps of all collected log entries, ensuring that all log data is time-stamped to a standard time regardless of the time zone and clock settings of the logging hosts. • LogRhythm directly supports testing procedure 10.5 by using discretionary access controls which allow restriction of the viewing of audit logs to individuals based on their role and Need-To-Know. LogRhythm protects audit trails from unauthorized modification by immediately archiving, hashing and storing collected logs in a secure central repository. LogRhythm includes an integrated file integrity monitoring which can ensure that the collection infrastructure is not tampered with. Additionally, LogRhythm servers utilize access controls at the operating system and application level to ensure log data cannot be modified or deleted. Alerts are customizable to prevent or allow alarms on a case-by-case basis, including not causing an alert with new data being added. Log Rhythm securely collect logs from the entire IT infrastructure including external-facing technologies for storage on an internal LAN Network where a LogRhythm appliance resides.

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		Segregation can be accomplished by allowing only log traffic to pass through LogRhythm via firewall, filter control on a router, or configuring the LogRhythm appliance's firewall to reject unanticipated connections. • LogRhythm directly supports testing procedure 10.6 by supplying a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily basis which provides an audit trail of who did what within LogRhythm and proof of log data review. • LogRhythm directly supports testing procedure 10.7 by automating the process of retaining audit trails. LogRhythm creates archive files of all collected log entries which are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on retention policy.
11. Regularly test security systems and processes	11.1.d, 11.4.b, 11.5.a, 11.5.b	LogRhythm meets or augments the following specific controls: • LogRhythm augments the testing process for procedure 11.1.d by providing alarms on the detection of rouge access points and also by providing details of detected rouge access points via investigations and reports. • LogRhythm provides alarms, investigations, reports, and tails to augment PCI-DSS control requirement 11.4. Collecting logs from network and host based IDS/IPS systems, its risk-based prioritization and alerting reduce the time and cost associated with monitoring and responding to IDS/IPS alerts. LogRhythm provides built-in alarms which can alert on IDS/IPS detected events such as attacks, compromises, denial of services, malware, reconnaissance activity, suspicious activity, and IDS/IPS signature update failures. LogRhythm provide details around these critical IDS/IPS events via investigations, reports, and tails.

REQUIREMENT	CONTROLS ADDRESSED	DESCRIPTION
		• LogRhythm directly supports testing procedure 11.5 by providing details of key integrity activity via investigations, reports, and tails on LogRhythm's File Integrity Monitor Agent. LogRhythm's File Integrity Monitor can be configured to monitor key file or directory activity, deletions, modification, and permission changes. The file integrity capability is completely automated, the agent can be configured to either scan for files or directory changes on a schedule or the kernel level driver can automatically detect file integrity activity in real-time.
12. Maintain a policy that addresses information security for employees and contractors	12.3.8, 12.3.9, 12. 9.5	LogRhythm meets or augments the following specific controls: • LogRhythm provides AIE rules, investigations, reports, and tails to support PCI-DSS control requirement 12.3 LogRhythm augments the testing process for 12.3 by providing alarms on vendor authentication failures and on vendor account accounts access granting. LogRhythm provides details on vendor account management activity, vendor authentication successes or failures, and remote session time outs via investigations and reports. • LogRhythm augments the testing process for 12.9 by providing real-time enterprise detection intelligence to address issues quickly to prevent damage and exposure. LogRhythm provides alarms and detail on security events such as attacks, compromises, denial of services, malware, reconnaissance activity, suspicious activity, and IDS/IPS signature update failures via investigations, reports, and tails.

Detailed PCI Applicability Matrix for VMware and LogRhythm

Table 4: PCI Applicability Matrix for VMware

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓		✓
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.		✓		✓	

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	1.1.3. b Verify that the current network diagram is consistent with the firewall configuration standards.			✓	✓	
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.	✓	✓	✓		✓
	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.	✓	✓	✓		✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					✓
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.	✓	✓		✓	✓
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit —deny allǁ or an implicit deny after allow statement.	✓	✓	✓	✓	✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.				✓	✓
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.		✓			
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.		✓	✓		✓
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.		✓	✓		✓
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only —establishedǁ 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.)		✓			

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.		✓	✓		
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.		✓	✓		
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.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.					
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 wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	2.1.1 Verify the following regarding vendor default settings for wireless environments:					
	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.			✓		

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.			✓		
	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.	✓		✓	✓	
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).	✓		✓	✓	

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.	✓		✓		
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.	✓	✓	✓	✓	✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓		✓	✓	
	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:					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓	✓	
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.		✓	✓		
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
	3.2.c For each item of sensitive authentication data below, perform the following steps:					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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		✓	✓		
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		✓	✓		

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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).		✓	✓		
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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 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.a Verify the existence of key-management procedures for keys used for encryption of cardholder data.					
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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 (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	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.					
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.					
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.					
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.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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.		✓			
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.		✓			

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.		✓			
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.	✓				
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.	✓				✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓				✓
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 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.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.	✓		✓	✓	✓
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.‖)	✓		✓	✓	
	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),	6.3.a Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.					
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.		✓			
	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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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:					
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.		✓	✓		
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.	✓	✓	✓		

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.	✓		✓		
	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.		✓			
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.		✓			

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.		✓			
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, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	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.					
	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.)					✓
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)					✓
6.5.6 All ―High‖ 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 ―High‖ vulnerabilities as identified in PCI DSS Requirement 6.2.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
For web applications and application interfaces (internal or external), the following additional requirements apply:						
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.		✓			✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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 controlǁ 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.	✓	✓	✓	✓	
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 allǁ 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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
7.2.3 Default —deny-all‖ 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-all‖ 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.	✓	✓	✓	✓	✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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.	✓	✓	✓	✓	

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.					
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:					
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.	✓	✓	✓	✓	✓
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.	✓	✓	✓	✓	
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.	✓	✓	✓	✓	✓
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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	✓	✓	✓	✓	✓
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓	✓	
	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.	✓	✓	✓	✓	

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓	✓	
	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.	✓	✓	✓	✓	✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓	✓	✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
	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).					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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 commercial storage facility. Review the location's security at least annually.	9.5.a Observe the storage location's physical security to confirm that backup media storage is secure.					
	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.					
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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.					
	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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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).					
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.	✓	✓	✓	✓	✓
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.	✓	✓	✓	✓	✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.	✓	✓	✓	✓	✓
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.	✓	✓	✓	✓	✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.	✓	✓	✓	✓	
	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.	✓	✓	✓	✓	

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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:					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.		✓	✓		✓
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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. 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.a Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.					
	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.					
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.					
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 occurred.	11.2 Verify that internal and external vulnerability scans are performed as follows:					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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 —High‖ vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.					
	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). 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	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.					
	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).					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
staff.	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 performed by internal staff.	11.2.3.a Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.					
	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 ―High‖ 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).					
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	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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
environment, or a web server added to the environment). These penetration tests must include the following:	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).					
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.					
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.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.					
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 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.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			✓		✓
	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).					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.					
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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					✓
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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.					
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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:					
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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.					
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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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:					
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 payment brands					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
	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.					
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.					
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.					✓

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	80
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.					
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.					

PCI REQUIREMENT	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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).	✓			✓	
	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	PCI TESTING PROCEDURES	VCLOUD SUITE	VCLOUD NETWORKING AND SECURITY SUITE	VCM (VCOPS SUITE)	VIEW	LOGRHYTHM
Number of PCI DSS Controls Addressed		104	116	113	80	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	✓	✓			
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 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 and contained in this document is for educational and informational purposes only. Coalfire makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire

Coalfire 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/FedRAMP.
For more information, visit www.coalfire.com.

Coalfire®

IT Governance, Risk & Compliance