

APPENDIX **B**

Verizon Business Reference Architecture Report—Cisco PCI Solution for Retail

Based on PCI DSS v. 2.0

06/24/2011

Table of Contents

Contact Information 2	
1. Executive Summary 2	
Architecture Description 2	
High Level Network Diagram 3	
Quarterly Vulnerability Scans 4	
2. Description of Scope of Work and Approach Taken	4
PCI DSS Version 4	
Timeframe 4	
Environment on which Assessment Focused 4	
Network Segmentation 5	
Exclusions 5	
Wireless LANs and/or Wireless Applications 6	
List of Individuals Interviewed 6	
Build and Maintain a Secure Network 7	
Protect Cardholder Data 36	
Maintain a Vulnerability Management Program 50	
Implement Strong Access Control Measures 62	

Regularly Monitor and Test Networks 89 Maintain an Information Security Policy 120

Contact Information



1. Executive Summary

Architecture Description

Cisco Systems, Inc engaged Verizon Business to conduct a PCI reference architecture assessment of their "PCI Solution for Retail" designed architecture, based on the PCI DSS v2.0 standard. The architecture assessment against the PCI DSS v2.0 standard included a review of the Cisco PCI Solution for retail network architecture, configurations, security applications, and web management consoles.

Cisco Systems, Inc. will continue to market the assessed reference architecture solution to retail customers looking to meet PCI requirements, specifically within their retail environment and within their back-end data center infrastructure. Cisco has used findings from the assessment to ensure configurations within their solution meet PCI requirements specific to their solution, and plan to provide the results of the assessment to Cisco Sales Engineers interfacing with retail customers.

Verizon Business' assessment covered three PCI retail architectures, targeted to small, medium, and large retail environments. Verizon Business found the three solution architectures to address several technical PCI requirements, and can address other requirements either as a compensating control, or in conjunction with compensating controls depending on organizations infrastructure requirements. The retail architectures are designed to be deployed within a POS retail location, with central management/logging components deployed in a data center environment.

As Cisco's PCI Solution for Retail architecture only addresses some aspects of a merchant's overall PCI compliance responsibility, several areas of PCI compliance are left to the merchant to obtain full compliance. The overall approach to the assessment was to focus validation efforts on components which are core to Cisco's PCI Solution for Retail environment. System components outside of the Cisco PCI Solution for Retail environment (e.g. corporate email, corporate Internet/DMZ firewalls, central cardholder databases, POS systems, mainframes, and corporate networks) were not included in the scope of the assessment.

High Level Network Diagram



Quarterly Vulnerability Scans

N/A - Quarterly scanning (internal and external) is the responsibility of the merchant/service provider, and was not part of the assessment.

2. Description of Scope of Work and Approach Taken

PCI DSS Version

PCI DSS v.2.0 was used for the reference architecture review.

Timeframe

The review took place through several remote interviews and remote validation:

• 3/1/2011-4/10/2011

Environment on which Assessment Focused

The architecture assessment included the following components:

- Cisco Routers (ISR)—891w-AGN, 1941w, ISR G2, 2921/51 ISR G2, 3945 ISR G2, ASR1000, and 7206VXR ISRs are configured with Firewall and IDS feature set.
- Cisco Switches—2960 PD-8TT-L, 2960- 8TC-L, 2960 S, 2960 C, 3560 C, 3560 X, 3750 X, 4507-Sup 7, 4948, 6500, Nexus1000v, Nexus5000, Nexus7000, MDS 9500
- MDS Switch Fabric
- Cisco Wireless —1262N Access Points, 3502E Access Points, 3502I Access Points, CT5508 Controller, WLC2125 Controller, Mobility Service Engine, WCS-Wireless Manager
- Cisco Security devices—ASA 5510, ASA 5540, ASA 5580, NAC, IOS Firewall, AnyConnect -VPN.
- Server Vitalization—Servers ISR SRE 900, UCS Express ESXi
- VBlock—UCS MDS EMC SAN
- Cisco Security Manager—Central provisioning of device configuration and security policies, including: ASAs, Cisco Firewall Services Modules, IDS, ISRs, and switches
- Cisco Secure Access Control Server (ACS)—AAA server
- LAN Management Solution (LMS)—Infrastructure Management
- **RSA Access Manager**—Used for central authentication/logging for access to RSA Data Protection Manager within the assessed environment.
- **RSA Authentication Manager**—Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
- RSA Data Protection Manager (formerly RSA Key Manager)

- **RSA enVision**—RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.
- **HyTrust**—Network-based virtual infrastructure policy enforcement. Administrative access control, enforcement of policy across virtual infrastructure, hypervisor hardening, and audit logging. Access and User administration, change and configuration, and operations
- EMC Ionix NCM—Built-in compliance template(s) for PCI (and other regulatory requirements). Detects "at-risk" devices according to published vulnerabilities

Network Segmentation

Cisco has designed three network architectures for small, medium, and large retail environments. Cisco has chosen Cisco Integrated Services Routers (ISRs) to provide firewall, IDS/, and routing functionality. Access-lists are applied through firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic to the PCI Solution for Retail; all traffic approved within each design is explicitly allowed to the IP address, port and service level. Additionally, Cisco has incorporated wireless into the design, using WPA-TKIP for secure wireless networking.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in all data center segments, including Cisco Firewall Services Module and ASA stateful firewall filtering and integrated IDS/ detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication.

All network devices within the PCI Solution for Retail are centrally managed through the following:

- Cisco Security Manager (CSM) (Central security management for ISRs and switches (e.g., firewall policy, IDS/signatures))
- Cisco Wireless Control System (WCS)—(Central wireless management)
- Cisco ACS—Central TACACS+ (central authentication) server for ASA firewall, Cisco Firewall Services Module, ISR, 7206 VXR router, switch, wireless controller (RSA enVision and WCS).
- RSA enVision—Central logging/Correlation/Analysis/Alerting server. Alerts from IDS/alerts and firewall logs.
- Cisco ASDM—Central configuration for ASA firewalls.
- Cisco Device Manager (IDM)—IDS/configuration management.

Exclusions

Due to the nature of this assessment, several areas of a normal PCI assessment were excluded, including:

- Central cardholder data storage
- Authorization/settlement processes
- Policies, procedures, and standards
- Assessment of "in transit" cardholder data
- · Physical security
- SDLC policies and procedures

• Live cardholder transactions (a POS environment, which includes authorization responses, was not available during the assessment)

Wireless LANs and/or Wireless Applications

Wireless networks within the PCI Solution for Retail environment have been configured to use WPA-TKIP authentication for secure wireless networking. All wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the PCI Solution for Retail network. Additionally, best practice security parameters have been applied to wireless networks, including: HTTPS access for wireless management, default SSID has been changed, SNMPv3 used (default strings changed), and HTTP access has been disabled.

List of Individuals Interviewed

The following staff was interviewed:

Interviewee(s)	Title
Christian Janoff, Bart Mcglothin	Network architecture, firewalls, routers, switches, wireless, IDS/
Christian Janoff, Bart Mcglothin	Audit Logging
Christian Janoff, Bart Mcglothin	Access Control / Authentication
Christian Janoff, Bart Mcglothin	CSM
Tom Hua	CSM
Christian Janoff, Bart Mcglothin	Wireless
Christian Janoff, Bart Mcglothin	LMS
Rupesh Chakkingal,	RSA Data Protection Manager
Rupesh Chakkingal	RSA Data Protection Manager
Bart Mcglothin	Cisco ASA – Secure configuration reviews
Sheri Spence	EMC SAN
Syed Ghayur	Nexus 1kv
Mike Adler	Wireless lab
Sujit Ghosh	Wireless lab
K. Sigel	HyTrust
R. Budko	HyTrust
Christian Janoff, Bart Mcglothin	Cisco Virtual Service Gateway
Syed Ghayur	Cisco Virtual Service Gateway
David Valiquette	RSA
Manual Kamer	EMC Ionix
Pandit Panburana	СИСМ
Mourad Cherfaoui	СИСМ

Danny Dhillon	RSA enVision
Danny Dhillon	RSA Authentication Manager
,	RSA Data Protection Manager, RSA Access Manager, RSA Authentication Manager

List of Documents Reviewed

The following documents were reviewed:

Document	Date
Enterprise Retail PCI DSS 2.0.pdf	11/17/2010
switch and router configs	04/15/11
Switch configs - stores	04/15/11
Common requirements questions across all devices.xls	12/01/10
Products Alignment_2010-10-13.xlsx	10/13/10
PCI Retail Solution Products.xlsx	04/15/11

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

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

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

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

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
 1.1 Establish firewall and router configuration standards that include the following: 1.1.1 A formal process 	 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 Verify that there 	N/A – Firewall/Router configuration		
for approving and testing all network connections and changes to the firewall and router configurations	is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	standards (documentation) is the responsibility of the merchant / service provider.		
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.	Verizon Business reviewed network diagrams and verified that they document all connections to cardholder data, including any wireless networks.		Note: Since each network environment will be unique to the merchant or service provider, updating network diagrams remains the responsibility of each merchant / service provider
	1.1.2.b Verify that the diagram is kept current.	Verizon Business reviewed network diagrams and verified that they kept current.		Note: Since each network environment will be unique to the merchant or service provider, updating network diagrams remains the responsibility of each merchant / service provider
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 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		

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.	 N/A - Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider. Note: Verizon Business confirmed role-based groups were created within Cisco ACS for logical management of network devices (e.g. Administrator, System Monitoring, and Config Manager groups). 	
 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.	 N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider. Note: Verizon Business reviewed access-lists, in addition to a documented list of required services/protocols for the PCI Solution for Retail environment, and confirmed traffic is limited to that which is required for the environment. 	
FOFS, IMAF, and SNPIF.	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.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.	
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.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.	
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.	

1.2 Build firewall and	1.2 Examine firewall		
router configurations	and router		
that restrict connections	configurations to verify		
between untrusted	that connections are		
networks and any	restricted between		
system components in	untrusted networks		
the cardholder data	and system		
environment.	components in the		
	cardholder data		
	environment, as		
Note: An "untrusted	follows:		
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	
1.2.1 Restrict inbound and outbound traffic to	1.2.1.a Verify that inbound and outbound	Verizon Business reviewed access lists across firewalls and routers and		Configurations for perimeter
that which is necessary	traffic is limited to that	verified that inbound and outbound		firewalls/routers
for the cardholder data	which is necessary for	traffic is limited to that which is		outside the PCI
environment.	the cardholder data environment, and that	necessary for a cardholder data environment.		Solution for Retail
	the restrictions are	Verizon Business observed		environment are
	documented.	system-generated configuration		the responsibility of merchant /
		output for the following system		service provider.
		components: Cisco ASA 5500 Series-data center		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5500 Series-store		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
	1.2.1.b Verify that all	Cisco 3945 Verizon Business reviewed access		
	other inbound and	lists across firewalls and routers and		
	outbound traffic is	verified that all other inbound and		
	specifically denied, for example by using an	outbound traffic is specifically denied.		
	explicit "deny all" or an	Verizon Business observed system-generated configuration		
	implicit deny after allow statement.	output for the following system		
	statement.	components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		

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.	Verizon Business reviewed router configuration and verified that configuration files are secure and synchronized. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206	
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.	Verizon Business confirmed that the PCI Reference Architecture for Retail Solutions was designed and segmented to require all wireless traffic destined for any wired host (WCS Manager), to pass through firewall access-lists before being permitted. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945	

			I	
1.3 Prohibit direct public	1.3 Examine firewall and router			
access between the Internet and any system	configurations—includi			
component in the	ng but not limited to			
cardholder data	the choke router at the			
environment.	Internet, the DMZ			
	router and firewall, the			
	DMZ cardholder segment, the perimeter			
	router, and the internal			
	cardholder network			
	segment—to determine that there is no direct			
	access between the			
	Internet and system			
	components in the			
	internal cardholder			
	network segment, as detailed below.			
1.3.1 Implement a DMZ	1.3.1 Verify that a DMZ	Verizon Business reviewed network		
to limit inbound traffic to	is implemented to limit	topologies and access lists across		
only system components	inbound traffic to only	firewalls and routers and verified that		
that provide authorized publicly accessible	system components that provide authorized	a DMZ is implemented to limit inbound traffic to only system		
services, protocols, and	publicly accessible	components that provide authorized		
ports.	services, protocols, and	publicly accessible services,		
	ports.	protocols, and ports.		
		Verizon Business observed		
		system-generated configuration		
		output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Services Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
	1		I	

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.	Verizon Business reviewed static IPs, and access lists across firewalls and routers and verified that that inbound Internet traffic is limited to IP addresses within the DMZ.	Perimeter firewall/router configurations and rule sets are the responsibility of the merchant
		Verizon Business observed system-generated configuration output for the following system components:	/ service provider.
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

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.	Verizon Business reviewed network diagrams, configurations from network-infrastructure system components, including wireless APs and verified that direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.	
		Verizon Business observed system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

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.	Verizon Business reviewed access-lists on the Internet edge router and confirmed that Internet sourced RFC-1918 addresses are explicitly denied and that internal addresses cannot pass from the Internet into the DMZ.	
		Verizon Business observed system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

1.3.5 Do not allow	1.3.5 Verify that	Verizon Business reviewed outbound	
unauthorized outbound	outbound traffic from	access-lists from the PCI Reference	
traffic from the	the cardholder data	Architecture for Retail Solutions	
cardholder data	environment to the	environment and confirmed that all	
environment to the Internet.	Internet is explicitly authorized	outbound traffic is destined for "data	
Internet.	authorized	center" systems. There is no outbound Internet access from the	
		PCI Reference Architecture for Retail	
		Solutions environment.	
		Verizon Business observed	
		system-generated configuration	
		output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5500 Series data center	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	1.3.6 Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are	Verizon Business confirmed the PCI Solution for Retail environment configurations for the Cisco ASA firewalls, Cisco Virtual Service Gateways, Cisco Firewall Services Modules, and ISRs with a firewall feature set were configured to perform stateful packet inspections.	
	associated with a previously established session.)	Verizon Business observed system-generated configuration output for the following system components:	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

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 untrusted networks.	1.3.7 Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	Verizon Business reviewed network topologies, network diagrams, and access lists across firewalls and routers and verified that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	
		Verizon Business observed system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	

1.3.8 Do not disclose private IP addresses and routing information to	1.3.8.a Verify that methods are in place to prevent the disclosure	Verizon Business reviewed DHCP reservations, static IPs, and access lists across firewalls and routers and	
unauthorized parties.	of private IP addresses	confirmed that RFC 1918 addresses	
Note: Methods to obscure IP addressing	and routing information from internal networks	were used within the PCI Solution for Retail environment.	
may include, but are not limited to:	to the Internet.	Verizon Business observed system-generated configuration	
Network Address Translation (NAT)		output for the following system components:	
Placing servers		Cisco ASA 5500 Series-data center	
containing cardholder		Cisco ASA 5585	
data behind proxy servers/firewalls or		Cisco ASA 5540	
content caches,		Cisco ASA 5500 Series-store	
Removal or filtering of		Cisco ASA 5510	
route advertisements for		Cisco Firewall Services Module	
private networks that employ registered		Cisco routers-store	
addressing,		Cisco 891W	
Internal use of		Cisco 1941W	
RFC1918 address space		Cisco 2921	
<i>instead of registered</i> <i>addresses.</i>		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.	N/A – Policies and procedures is the responsibility of the merchant / service provider.	

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.	N/A – Security Policy (Remote Access – Desktop firewalls) is the responsibility of the merchant / service provider. Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the merchant / service provider network, is the responsibility of the merchant / service provider.	
	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	 N/A - Security Policy (Remote Access - Desktop firewalls) is the responsibility of the merchant / service provider. Installation of personal firewall software for any mobile and employee-owned computers with 	
	employee-owned computers.	direct Internet connectivity, and which are used to access the merchant / service provider network, is the responsibility of the merchant / service provider.	

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

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

PCI DSS	Testing Procedures	In Place	Not in Place	Comments
Requirements 2.1 Always change vendor-supplied defaults 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	Verizon Business observed administrators during the login process, while attempting to logon with default accounts and passwords. Verizon Business confirmed all default passwords, including passwords for interactive administrator accounts and SNMP community strings have been changed. Verizon Business confirmed all default administrator accounts have been removed, where possible. Some default administrator accounts cannot be removed from the system, due to application dependencies; however, unique administrator accounts have been created, in order to eliminate the need to use all default administrator accounts.		
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 	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: Default SNMP community strings have been changed and (SNMPv3 is being used).		

2.1.1.c Verify defaul passwords/passphras access points were cl	ses on settings within the PCI Reference
	No default passwords exist within the wireless environment. These are entered at initial login. Only unique, non-default accounts exist for interactive administration within the wireless
2.1.1.d Verify firmw. wireless devices is up support strong encry authentication and transmission over wi	bdated to settings within the PCI Reference ption for Architecture for Retail Solutions environment and verified the
networks.	WPA technology is enabled (WPA/TKIP w/PEAP authentication).
2.1.1.e Verify other security-related wire vendor defaults were if applicable.	-
	No Default SSID exists. This must be entered at initial installation, and is recommended by Cisco to be unique.
	SSID broadcast was disabled.
	Wireless management and web mode is disabled.

2.2 Develop	2.2.a Examine the	N/A – System configuration standards	
configuration	organization's system	(e.g. Firewall/Router standards, server	
standards for all	configuration standards for all	standards, wireless standards) is the	
system	types of system components	responsibility of the merchant / service	
components.	and verify the system	provider.	
Assure that these	configuration standards are	Verizon Business observed system-generated configuration	
standards address	consistent with	output for the following system	
all known		components:	
	industry-accepted hardening	Cisco ASA 5500 Series-data center	
security	standards.	Cisco ASA 5585	
vulnerabilities and		Cisco ASA 5550	
are consistent		Cisco ASA 5500 Series-store	
with			
-		Cisco ASA 5510	
industry-accepted		Cisco Virtual Service Gateway	
system hardening		Cisco Firewall Services Module	
standards.		Cisco routers-store	
Sources of		Cisco 891W	
industry-accepted		Cisco 1941W	
system hardening		Cisco 2921	
standards may		Cisco 2951	
include, but are not		Cisco 3945	
limited to:		Cisco routers-data center	
		Cisco ASR 1002	
Center for Internet		Cisco 7206	
Security (CIS)		Cisco switches-data center	
International		Cisco Catalyst 6509	
Organization for		Cisco Catalyst 4948	
Standardization		Cisco Nexus 7010	
		Cisco Nexus 5020	
(ISO)		Cisco switches-store	
SysAdmin Audit		Cisco Catalyst 2960	
Network Security		Cisco Catalyst 2960G	
(SANS) Institute		Cisco Catalyst 2960PD	
. ,		Cisco Catalyst 2960CPD	
National Institute		Cisco Catalyst 2960S	
of Standards		Cisco Catalyst 25005	
Technology (NIST)		Cisco Catalyst 3560Z	
		Cisco Catalyst 3560CPD	
		Cisco Catalyst 3750X	
		Cisco Catalyst 4507+R	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		AIR-LAP1262N	
		EMC Ionix Network Configuration Manager	
		RSA Authentication Manager	
		RSA EnVision	
		Cisco Identity Services Engine	
		EMC CLARIION CX-240	
		Cisco Unified Computing System	
		Cisco UCS Express on Services Ready	
		Engine	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
		Note: Verizon Business reviewed configurations across all above mentioned	
		technologies and confirmed they were	
		configured according to best practice standards.	
		standal doi	

		1
2.2.b Verify that system	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards), is the	
configuration standards are	standards, wireless standards) is the	
updated as new vulnerability	responsibility of the merchant / service provider.	
issues are identified, as	Verizon Business observed	
defined in Requirement	system-generated configuration	
6.2.	system-generated configuration output for the following system	
	components:	
	Cisco ASA 5500 Series-data center	
	Cisco ASA 5585 Cisco ASA 5540	
	Cisco ASA 5500 Series-store Cisco ASA 5510	
	Cisco Virtual Service Gateway	
	Cisco Firewall Services Module	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W	
	Cisco 2921	
	Cisco 2921 Cisco 2951	
	Cisco 3945	
	Cisco routers-data center	
	Cisco ASR 1002	
	Cisco 7206	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco switches-store	
	Cisco Catalyst 2960	
	Cisco Catalyst 2960G	
	Cisco Catalyst 2960PD	
	Cisco Catalyst 2960CPD	
	Cisco Catalyst 2960S	
	Cisco Catalyst 3560E	
	Cisco Catalyst 3560X	
	Cisco Catalyst 3560CPD	
	Cisco Catalyst 3750X	
	Cisco Catalyst 4507+R	
	HyTrust Appliance	
	Cisco Unified Wireless	
	AIR-CT5508	
	MSE3550 Cisco WCS Manager	
	AIR-CAP1042N	
	AIR-CAP3502i	
	AIR-CAP3502E	
	AIR-LAP1262N	
	EMC Ionix Network Configuration Manager	
	RSA Authentication Manager	
	RSA EnVision	
	Cisco Identity Services Engine	
	EMC CLARIION CX-240	
	Cisco Unified Computing System	
	Cisco UCS Express on Services Ready Engine	
	Cisco Secure Access Control Server	
	Cisco Video Surveillance	
	Cisco Physical Access Control	
	Note: Verizon Business reviewed	
	configurations across all above mentioned	
	technologies and confirmed they were configured according to best practice	
	standards.	
	•	· ·

2.2.c Verify that system configuration standards are applied when new systems are	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service	
configured.	provider.	
	Verizon Business observed system-generated configuration output for the following system	
	components: Cisco ASA EEOO Sorios (Data Contor)	
	Cisco ASA 5500 Series (Data Center) Cisco ASA 5500 Series (Store)	
	Cisco Virtual Service Gateway	
	Cisco Firewall Services Module	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W	
	Cisco 2921 Cisco 2951	
	Cisco 3945	
	Cisco routers-data center	
	Cisco ASR 1002	
	Cisco 7206	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco switches-store	
	Cisco Catalyst 2960	
	Cisco Catalyst 2960G	
	Cisco Catalyst 2960PD	
	Cisco Catalyst 2960CPD	
	Cisco Catalyst 2960S Cisco Catalyst 3560E	
	Cisco Catalyst 35602	
	Cisco Catalyst 3560CPD	
	Cisco Catalyst 3750X	
	Cisco Catalyst 4507+R	
	HyTrust Appliance	
	Cisco Unified Wireless	
	AIR-CT5508	
	MSE3550	
	Cisco WCS Manager	
	AIR-CAP1042N AIR-CAP3502i	
	AIR-CAP3502E	
	AIR-LAP1262N	
	EMC Ionix Network Configuration Manager	
	RSA Authentication Manager	
	RSA EnVision	
	Cisco Identity Services Engine	
	EMC CLARIION CX-240	
	Cisco Unified Computing System	
	Cisco UCS Express on Services Ready Engine	
	Cisco Secure Access Control Server	
	Cisco Video Surveillance	
	Cisco Physical Access Control	
	Note: Verizon Business reviewed configurations across all above mentioned	
	technologies and confirmed they were configured according to best practice	
	standards.	
	•	

	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).		
2.2.1 Implement only one primary function per server to prevent functions that	2.2.1.a For a sample of system components, verify that only one primary function is implemented per server.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider.	
require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS		Note: Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.	
should be implemented on separate servers.)	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider.	
Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	,,		

2.2.2 Enable only	2.2.2.a For a sample of	Verizon Business reviewed configuration settings for PCI Reference Architecture for Retail	•
necessary and	system components, inspect enabled system services,	Reference Architecture for Retail	
secure services, protocols,	daemons, and protocols.	Solutions and verified that that only necessary services or protocols are	
daemons, etc., as	Verify that only necessary	enabled.	
required for the	services or protocols are	Note: Although Cisco followed a	
function of the	enabled.	configuration standard to harden the OS for management consoles, Verizon Business did not review those	
system.		Business did not review those configurations beyond secure	
Implement security		administrative access (e.g. https,	
features for any		administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the merchant / service provider, and would vork clarification of the provider of the	
required services,		hardening is the responsibility of the	
protocols or		I WOULD VALV SIGHTICATION, DEDENDING OF	
daemons that are		OS platform and POS applications deployed.	
considered to be			
insecure—for		Verizon Business observed system-generated configuration	
example, use		output for the following system components:	
secured technologies such		Cisco ASA 5500 Series-data center	
as SSH, S-FTP,		Cisco ASA 5585	
SSL, or ec VPN to		Cisco ASA 5540	
protect insecure		Cisco ASA 5500 Series-store	
services such as		Cisco ASA 5510	
NetBIOS,		Cisco Virtual Service Gateway	
file-sharing, Telnet,		Cisco Firewall Services Module	
FTP, etc.		Integrated Services Routers (ISRs)	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N AIR-CAP3502i	
		AIR-CAP3502E	
		AIR-LAP1262N	
		EMC Ionix Network Configuration	
		Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services Engine	
		Cisco UCS Express on Services Ready	
		Engine	
		Cisco Unified Communications Manager	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

	2.2.2.b Identify any enabled	Verizon Business reviewed configuration settings for PCI	
	insecure services, daemons,	Reference Architecture for Retail	
	or protocols. Verify they are	Solutions and verified that insecure	
	justified and that security	services and protocols are not used.	
	features are documented and	Note: Although Cisco followed a configuration standard to harden the	
	implemented.	OS for management consoles, Verizon	
		Business did not review those configurations beyond secure	
		administrative access (e.g. https,	
		SSH), audit logging, and password/lockout settingsOS	
		hardening is the responsibility of the	
		hardening is the responsibility of the merchant / service provider, and would vary significantly, depending on	
		OS platform and POS applications	
		deployed.	
		Verizon Business observed	
		system-generated configuration output for the following system	
		components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Integrated Services Routers (ISRs)	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		AIR-LAP1262N	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco UCS Express on Services Ready	
		Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
L		· ·	1 1

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.	Verizon Business interviewed administrators, architects, and SMEs from business units to verify they have knowledge of common security parameters of the system components within the PCI Reference Architecture for Retail Solutions environment.		
----------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

2.2.3.b Verify that common security parameter settings	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service	Documentation and
are included in the system configuration standards.	responsibility of the merchant / service provider.	implementation of system configuration
	Verizon Business observed system-generated configuration output for the following system components:	standards is the responsibility of the merchant / service
	Cisco ASA 5500 Series-data center	provider.
	Cisco ASA 5585	F
	Cisco ASA 5540	
	Cisco ASA 5500 Series-store	
	Cisco ASA 5510	
	Cisco Virtual Service Gateway	
	Cisco Firewall Services Module	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W	
	Cisco 2921	
	Cisco 2951	
	Cisco 3945	
	Cisco routers-data center	
	Cisco ASR 1002	
	Cisco 7206	
	Cisco MDS Storage Switches	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco Security Manager (CSM)	
	HyTrust Appliance	
	Cisco Unified Wireless	
	AIR-CT5508	
	MSE3550	
	Cisco WCS Manager	
	AIR-CAP1042N AIR-CAP3502i	
	AIR-CAP3502I AIR-CAP3502E	
	AIR-LAP1262N	
	EMC Ionix Network Configuration Manager	
	EMC CLARIION CX-240	
	RSA Authentication Manager	
	RSA Data Protection Manager	
	RSA enVision	
	Cisco Identity Services Engine	
	Cisco UCS Express on Services Ready Engine	
	Cisco Unified Communications Manager and IP Phones	
	Cisco Unified Computing System (UCS)	
	Cisco Video Surveillance	
	Cisco Physical Access Control	

2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	 		_
bat common security parameters are set appropriately. Reference Architecture for Retail Solutions and confirmed they were and solutions and confirmed they were and solutions and confirmed they were and solutions and confirmed they were and appropriately. Were set appropriately. Vention Business also confirmed all system components, is the they fight they for an they https:/fight.theryption RDP) and they they fight.they for an they administration of the PCI Reference administration of the PCI Reference System generated configuration of the DCI Reference System generated configuration of the DCI Reference Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5500 Cisco Virtual Service Gateway Cisco Firwall Services Module Cisco Orders-store Cisco 3941 Cisco 3941 Cisco 3945 Cisco ASR 1002 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7020 Cisco N	2.2.3.c For a sample of	Verizon Business reviewed	Server
appropriately. Hit common security parameters business also confirmed all zoon management consoles were configured to support secure access (e.g. SSH http:/filet.and other insecure provider. business observed system control of the PCT Reference Architecture for Retail Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5500 Cisco Virtual Service Gateway Cisco 1941W Cisco 2921 Cisco ASA 5500 Cisco ASA 5500 Cisco ASA 5500 Cisco 3945 Cisco ASA 500 Cisco ASA 500 Cisco ASA 500 Cisco ASA 500 Cisco ASA 500 Cisco ASA 500 Cisco SSH Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Virtual Services Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Virtual Service Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7020 Cisco Nexus 7010 Cisco Nexus 7010 Ci		Reference Architecture for Retail	
appropriately. Heat Common Security Parameters business also confirmed all zoon management consoles were configured of support secure access (e.g. SSH https:/High-Encryption RDP) and that http:/High-Encryption RDP) and that http:/High-Encryption output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Cisco MSUM Cisco 1941W Cisco 2951 Cisco 3945 Cisco Oracles-data center Cisco ASA 1002 Cisco XDP Storage Switches Cisco Nexus 7010 Cisco	,	Solutions and confirmed they were	5
management consoles were control of all system to support secure access to Onigined to support secure access had been protocols commonly used for administrative access had been administrative access had been administr	•	that common security parameters	
management consoles were contigured to support secure access to contigue the support secure access to have a secure protocols commonly used for administrative access had been administrative access hadministrative access administrative access had be	appropriately.	were set appropriately. Verizon	,
to support secure access (e.g. SSH, dimensional system) https://teline.incomposition.components; http://teline.accomposition.components; http://teline.accomposition.components; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://teline.accomponents; http://te		manadomont concolos woro contidurod	5
Inter, reflect, and obtine hiseful e providers and the provider of the methods o		to support secure access (e.g. SSH,	
protocols commonly used for administrative access had beared disabled. Additionally, role-based disabled. Additionally, role-based administration of the PCP Reference Architecture for Retal Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco ASA 5510 Cisco ASA 5510 Cisco Firewall Services Module Cisco Firewall Services Module Cisco Firewall Services Module Cisco 2921 Cisco 2921 Cisco 2921 Cisco 2945 Cisco ASA 5100 Cisco 70441W Cisco 2921 Cisco 3945 Cisco aSA 500 Cisco Touters-data center Cisco 3945 Cisco Touters-data center Cisco ASA 5100 Cisco 2021 Cisco 2921 Cisco 2945 Cisco ASR 1002 Cisco 2026 Cisco Switches-data center Cisco ASR 1002 Cisco Catalyst 4500 Cisco Catalyst 4509 Cisco Catalyst 4509 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Catalyst 4948 Cisco Nexus 5020 Ci		https, High-Encryption RDP), and that	
disabled. Additionally, role-based administration of the PCT Reference Architecture for Retail Solutions. Verizon Business observed system-generated configuration output for the following System components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco ASA 5510 Cisco ASA 5510 Cisco ISCO Virtual Services Gateway Cisco Firewall Services Module Cisco Virtual Services Module Cisco Virtual Services Module Cisco 2921 Cisco 2921 Cisco 2951 Cisco 3945 Cisco 3945 Cisco 7206 Cisco Touters-data center Cisco 3945 Cisco Storage Switches Cisco Storage Switches Cisco Storage Switches Cisco Storage Switches Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		protocols commonly used for	
administration was configured for administration of the PCT Reference Architecture for Retail Solutions. Verizon Business observed system-generated configuration output for the following System components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco ASA 5510 Cisco SAS 5510 Cisco SAS 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 291W Cisco 2921 Cisco 2951 Cisco 3945 Cisco aSR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco MDS Storage Switches Cisco MDS Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		administrative access had been	
Architecture for Retail Solutions.serviceVerizon Business observed system-generated configuration output for the following system components:provider.Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540Cisco ASA 5585 Cisco ASA 5510Cisco ASA 5500 Series-store Cisco ASA 5510Cisco ASA 5510Cisco Firewall Services Module Cisco ASA 5510Cisco Firewall Services ModuleCisco Firewall Services Module Cisco 1941W Cisco 2951 Cisco 3945Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020Service ServiceCisco Nexus 7010 Cisco Nexus 5020Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified WirelessService Service		administration was configured for	
Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Cisco ASA 5500 Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Service Gateway Cisco Firewall Service Smotule Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2921 Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco 7206 Cisco ASR 1002 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Security Manager (CSM)		administration of the PCI Reference	,
system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5505 Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco Vitual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2945 Cisco routers-data center Cisco ASA 500 Cisco ASA 1002 Cisco ASA 500 Cisco MDS Storage Switches Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless			
Components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Virtual Services Module Cisco Virtual Services Module Cisco Reveal Services Module Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco ASS 1002 Cisco MSS torage Switches Cisco witches-data center Cisco Catalyst 6509 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Verizon Business observed system-generated configuration	provider.
Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 1941W Cisco 2951 Cisco 2921 Cisco 2921 Cisco 3945 Cisco 7206 Cisco 7206 Cisco ASA 5500 Cisco ASA 5510 Cisco ASA 5510 Cisco 7206 Cisco ASA 5510 Cisco ASA 5510 Cisco 7206 Cisco MSS Storage Switches Cisco Switches-data center Cisco Switches-data center Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		output for the following system	
Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5510 Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2951 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		•	
Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Services Module Cisco Firewall Services Module Cisco Firewall Services Module Cisco 7004 Cisco 70141W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2951 Cisco 2951 Cisco 7206 Cisco ASR 1002 Cisco 7206 Cisco Switches-data center Cisco Switches-data center Cisco Satalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASA 5500 Series-data center	
Cisco ASA 5500 Series-store Cisco Virtual Service Gateway Cisco Virtual Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco ASR 1002 Cisco 7206 Cisco MSS Storage Switches Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASA 5585	
Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASA 5540	
Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2951 Cisco 3945 Cisco a945 Cisco routers-data center Cisco 3945 Cisco routers-data center Cisco 7206 Cisco MDS Storage Switches Cisco Storage Switches Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASA 5500 Series-store	
Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASA 5510	
Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco Virtual Service Gateway	
Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco 7206 Cisco 7206 Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco Firewall Services Module	
Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco routers-store	
Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 891W	
Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco 7206 Cisco Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 1941W	
Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 2921	
Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 2951	
Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 3945	
Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco routers-data center	
Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco ASR 1002	
Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco 7206	
Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		Cisco MDS Storage Switches	
Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless		5	
Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless			
Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless			
Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless			
Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless			
HyTrust Appliance Cisco Unified Wireless			
Cisco Unified Wireless			
MSE3550			
Cisco WCS Manager			
AIR-CAP1042N			
AIR-CAP3502i			
AIR-CAP3502E			
AIR-LAP1262N			
EMC Ionix Network Configuration Manager		EMC Ionix Network Configuration	
EMC CLARiiON CX-240			
RSA Authentication Manager			
RSA Data Protection Manager		_	
RSA enVision		5	
Cisco Identity Services Engine			
<u>Cisco UCS Express on Services Ready</u>			
Engine		Engine	
Cisco Unified Communications Manager and IP Phones			
		-	
Cisco Unified Computing System (UCS)			
Cisco Video Surveillance			
Cisco Physical Access Control	 	Cisco Physical Access Control	

2.2.4 Domovio all	224 a Earla comple of	Varizan Rusinges reviewed	[]	Sonior
2.2.4 Remove all	2.2.4.a For a sample of system components, verify	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and		Server hardening,
unnecessary functionality, such	that all unnecessary	Architecture for Retail Solutions and		including
as scripts, drivers,	functionality (for example,	verified that they were based on best practice standards, and that all		appropriate
features,	scripts, drivers, features,	unnecessary functionality was		security
subsystems, file	subsystems, file systems, etc.)	disabled.		settings for
systems, and	is removed.	Verizon Business observed system-generated configuration output for the following system		all system
unnecessary web	is removed.	output for the following system		components,
servers.		components:		is the
		Cisco ASA 5500 Series-data center		responsibility
		Cisco ASA 5585		of the
		Cisco ASA 5540		merchant /
		Cisco ASA 5500 Series-store		service
		Cisco ASA 5510		provider.
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager (CSM)		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		AIR-LAP1262N		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine Cisco UCS Express on Services Ready		
		Engine Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System (UCS)		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

2.2.4.b. Verify enabled	Verizon Business reviewed configurations across all PCI Reference	Server
functions are documented an support secure configuration	Architecture for Refail Solutions and	hardening, including
Support Secure comparation	documented and support secure	appropriate
	configuration.	security
	Verizon Business observed	settings for all
	system-generated configuration output for the following system	system
	components:	components,
	Cisco ASA 5500 Series-data center	is the
	Cisco ASA 5585	responsibility
	Cisco ASA 5540	of the
	Cisco ASA 5500 Series-store	merchant / service
	Cisco ASA 5510	provider.
	Cisco Virtual Service Gateway	provider.
	Cisco Firewall Services Module	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W	
	Cisco 2921	
	Cisco 2951	
	Cisco 3945	
	Cisco routers-data center Cisco ASR 1002	
	Cisco 7206	
	Cisco MDS Storage Switches	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco Security Manager (CSM)	
	HyTrust Appliance	
	Cisco Unified Wireless	
	AIR-CT5508	
	MSE3550	
	Cisco WCS Manager	
	AIR-CAP1042N	
	AIR-CAP3502i	
	AIR-CAP3502E	
	AIR-LAP1262N	
	EMC Ionix Network Configuration Manager	
	EMC CLARIION CX-240	
	RSA Authentication Manager	
	RSA Data Protection Manager	
	RSA enVision	
	Cisco Identity Services Engine	
	Cisco UCS Express on Services Ready Engine	
	Cisco Unified Communications Manager and IP Phones	
	Cisco Unified Computing System (UCS)	
	Cisco Secure Access Control Server	
	Cisco Video Surveillance	
	Cisco Physical Access Control	

2.2.4.c . Verify that only documented functionality is	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and	Server hardening,
present on the sampled system components.	confirmed that only documented functionality is present on the sampled system components.	including appropriate security
	Verizon Business observed system-generated configuration output for the following system components:	settings for all system components,
	Cisco ASA 5500 Series-data center	is the
	Cisco ASA 5585	responsibility
	Cisco ASA 5540	of the
	Cisco ASA 5500 Series-store	merchant /
	Cisco ASA 5510	service
	Cisco Virtual Service Gateway	provider.
	Cisco Firewall Services Module	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W Cisco 2921	
	Cisco 2921 Cisco 2951	
	Cisco 3945	
	Cisco routers-data center	
	Cisco ASR 1002	
	Cisco 7206	
	Cisco MDS Storage Switches	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco Security Manager (CSM)	
	HyTrust Appliance	
	Cisco Unified Wireless	
	AIR-CT5508 MSE3550	
	Cisco WCS Manager	
	AIR-CAP1042N	
	AIR-CAP3502i	
	AIR-CAP3502E	
	AIR-LAP1262N	
	EMC Ionix Network Configuration Manager	
	EMC CLARIION CX-240	
	RSA Authentication Manager	
	RSA Data Protection Manager	
	RSA enVision	
	Cisco Identity Services Engine	
	Cisco Virtual Service Gateway	
	Cisco UCS Express on Services Ready Engine	
	Cisco Unified Communications Manager and IP Phones	
	Cisco Unified Computing System (UCS)	
	Cisco Secure Access Control Server	
	Cisco Video Surveillance	
	Cisco Physical Access Control	

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:			
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------	--	--	--
2.3.a Observe an	Verizon Business reviewed	Note:		
--------------------------------	-----------------------------------------------------------------------------------------------------------	---------------------------		
administrator log on to each	non-console administrative access for	Verification of		
system to verify that a strong	all PCI Reference Architecture for Retail Solutions and verified that	telnet		
encryption method is invoked	Retail Solutions and verified that strong encryption methods are invoked before the administrator's	presence		
before the administrator's	password is requested.	within the		
password is requested.	Verizon Business observed	management		
	system-generated configuration output for the following system	consoles		
	components:	(Windows		
	Cisco ASA 5500 Series-data center	Server 2003)		
	Cisco ASA 5585	was not		
	Cisco ASA 5540	performed. This is the		
	Cisco ASA 5500 Series-store	responsibility		
	Cisco ASA 5510	of the		
	Cisco Virtual Service Gateway	merchant /		
	Cisco Firewall Services Module	service		
	Cisco routers-store	provider, as		
	Cisco 891W	part of secure		
	Cisco 1941W	configuration		
	Cisco 2921	standard		
	Cisco 2951	processes.		
	Cisco 3945			
	Cisco routers-data center			
	Cisco ASR 1002			
	Cisco 7206			
	Cisco MDS Storage Switches			
	Cisco switches-data center			
	Cisco Catalyst 6509			
	Cisco Catalyst 4948			
	Cisco Nexus 7010			
	Cisco Nexus 5020			
	Cisco Security Manager (CSM)			
	HyTrust Appliance			
	Cisco Unified Wireless			
	AIR-CT5508			
	MSE3550			
	Cisco WCS Manager			
	AIR-CAP1042N			
	AIR-CAP3502i			
	AIR-CAP3502E			
	AIR-LAP1262N			
	EMC Ionix Network Configuration Manager			
	EMC CLARIION CX-240			
	RSA Authentication Manager			
	RSA Data Protection Manager			
	RSA enVision			
	Cisco Identity Services Engine			
	Cisco Virtual Service Gateway			
	Cisco UCS Express on Services Ready			
	Engine Cisco Unified Communications Manager and IP Phones			
	-			
	Cisco Unified Computing System (UCS)			
	Cisco Secure Access Control Server			
	Cisco Video Surveillance			
	Cisco Physical Access Control			

2.3.b Review services and parameter likes on system rules on the tenet and other remote login commands are not available for use internally. Verication Subjects reviewed system of tenet within the function of tenet of tenet internally. Verication Subjects rules and verified that the function of tenet of tenet of tenet internally. Verication Subjects and verified that the function of tenet of	 3 h Roview convices and	Varizon Business reviewed	Note:
all PLI Reterines Architecture for other remote login commands are not available for use internally.	.3.b Review services and	non-console administrative access for	Note: Verification of
ther remote login commands are not xavailable for use internally. Server 2003) Server 2003 Crsco ASA 5500 Series-data center Clsco ASA 5510 Clsco ASA 5500 Clsco Class 454 Clsco ASA 5500 Clsco Class 454 Clsco ASA 500 Clsco Class 454 Clsco Nexus 5020 Clsco ASA AS020 Clsco Virtual Service Clso MARCAT300 MARCAT300 MARCAT300 MARCAT300 Clsco Virtual Service Clso MARCAT300 MARCAT300 Clsco Virtual Service Gateway Clsco Virtual Service Gateway Clsco Virtual Service Clsco MARCAT300 MARCAT300 Clsco Virtual Service Clsco MARCAT300 Clsco Virtual Service Clsco MARCAT300 Clsco Virtual Service Clsco MARCAT300 Clsco Virtual Service Clsco MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 Clsco Virtual Service Clsco MARCAT300 Clsco Virtual Service Clsco MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300 MARCAT300		all PCI Reference Architecture for	
are not available for use internally. commands are not available for use internally. cross Desiness observed vericon Business observed vericon Business observed vericon Business observed components: Clisco ASA 5500 Series-data center Clisco ASA 5500 Series-store Clisco 450 A510 Clisco 1941W Clisco 1941W Clisco 1941W Clisco 1941W Clisco 2921 Clisco 2921 Clisco 7206 Clisco 7206 Clisco 7206 Clisco ASA 1002 Clisco Clashyst 6509 Clisco Clashyst 6509 Clisco Clashyst 4948 Clisco Nexus 5020 Clisco Clashyst 6509 Clisco Clashyst 6509 Clisco Clashyst 6509 Clisco Clashyst 4948 Clisco Nexus 5020 Clisco Clashyst 6509 Clisco Nexus 5020 Clisco Nex		Telnet and other remote login	
internally. intern		commands are not available for use	•
system-cenerated configuration of types components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco Nituel Service Gateway cisco Piewall Service Setway Cisco 1941 W Cisco 1941 W Cisco 1941 W Cisco 1941 W Cisco 2921 Cisco 2921 Cisco 2921 Cisco 7006 Cisco Touters-store Cisco 7006 Cisco Touters-data center Cisco 7006 Cisco Touters-data center Cisco 7006 Cisco Nexus 5009 Cisco Catalyst 6509 Cisco Nexus 5020 Cisco Nexus		,	
components:Server 2003) was notCisco ASA 5500 Series-data centerServer 2003)Cisco ASA 5500 Series-storePerformed.Cisco ASA 5510This is theCisco ASA 5510of theCisco Virtual Service Gatewaymerchant /Cisco Tuters-storeprovider, aspart of secureconditional servicesCisco 2921standardCisco ASA 500cisco 2921Cisco ASA 500standardCisco 2921standardCisco 29251cisco 2921Cisco ASA 500cisco 2921Cisco ASA 1002Cisco 2921Cisco ASA 1002Cisco Catalyst 6509Cisco Catalyst 6509Cisco Catalyst 4509Cisco Nexus 5020Cisco Nexus 5020Cisco Catalyst 4508MiteressAire-Cr508MiscasoMiscasoMiscasoAire-CatalianceCisco WeresCisco Weres ManagerAire-CatalianAire-CatalianceCisco WeresCisco Unified WirelessAire-CatalianAire-CatalianMiscasoAire-CatalianMiscasoManagerRSA Authentication ManagerRSA Data Protection ManagerRSA Authentication ManagerRSA Data Protection ManagerCisco Uified Communications Manager and PhonesesCisco Uified Communications Manager and PhonesesCisco Video Survie Screes Cataly EngineCisco Uified Communications Manager and PhonesesCisco Video Survie ScreesCisco Uified Communications Manager and PhonesesCisco Video Survie Sirvee	·	system-generated configuration	9
Cisco ASA 5500 Series-data centerServer 2003)Cisco ASA 5585performed.Cisco ASA 5540This is theCisco ASA 5510of theCisco ASA 5510of theCisco ASA 5510of theCisco Cisco Virtual Service Gatewaymerchant /Cisco Cisco Virtual Services Moduleprovider, asCisco 2011cisco 2921Cisco 2921provider, asCisco 2921cisco 2921Cisco 704Ers-data centercisco 2921Cisco Catalyst 6509cisco 2921Cisco Catalyst 6509cisco 2020Cisco Catalyst 6509cisco 2020Cisco Security Manager (CSM)HyTrust ApplianceCisco Wexus 5020Cisco Security ManagerAIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021Cisco Unified WirelessAIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021AIR-CAP35021 <td< td=""><td></td><td>output for the following system</td><td>(Windows</td></td<>		output for the following system	(Windows
Cisco ASA 5585 performed. Cisco ASA 5540 This is the Cisco ASA 5510 Series-store performed. This is the Cisco SAS 5510 of the Cisco Virtual Service Gateway perchant / Cisco Firewall Service Module perchant / Cisco Firewall Service Module perchant / Cisco Firewall Service Gateway perchant Cisco 691W part of secure Cisco 691W constraint Cisco 2921 constraint Cisco 2921 constraint Cisco 2921 constraint Cisco 3945 Cisco 7006 Cisco 7006 Cisco 7006 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Catalyst 4948 Cisco Nexus 5020 Cisco Cisco Vieness AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 AIR-CAPI3020 Cisco Cisco		•	Server 2003)
Cisco ASA 5540 The control of the co			
Cisco ASA 5500 Series-store responsibility Cisco Virtual Service Gateway of the Cisco Virtual Service SModule provider, as Cisco 191W Service SModule configuration Cisco 1941W Configuration Cisco 1941W Configuration Cisco 2921 processes. Cisco 2921 Cisco 2925 Cisco Touters-data center Cisco 3945 Cisco 7206 Cisco Nexus 7010 Cisco Catalyst 4509 Cisco Secure Ada Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Wireless AIR-CATS08 MSE3500 Cisco Wireless AIR-CATS08 MSE3502 Cisco Wireless AIR-CATS08 MSE3502 Cisco Wireless AIR-CATS08 MSE3502 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Security Manager (CSM) HyTrust Appliance Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Wireless AIR-CATS08 MSE3500 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Security Manager (CSM) HyTrust Appliance Cisco Wireless AIR-CATS08 MSE3500 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Security Manager (CSM) HyTrust Appliance Cisco Wireless AIR-CATS08 MSE3500 Cisco Catalyst 6509 Cisco Catalyst 65			•
Cisco ASA 5510 of the merchant / Cisco Virtual Service Gateway merchant / Cisco Firewall Services Module service provider, as provider, as provider, as provider, as processes. Cisco 1941W standard Cisco 2951 Cisco 2951 Cisco 3945 Cisco 7206 Cisco ASR 1002 Cisco ASR 1002 Cisco 7206 Cisco 7206 Cisco 7206 Cisco 7206 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco WCS Manager AIR-CAT508 MS23530 Cisco WCS Manager AIR-CA7500 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 AIR-CA75002 Cisco Victo Stronger Cisco Cisco WCS Manager Cisco Victo Stronger Cisco Cisco Manager Cisco Unified Virue Service Sentemay Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Virue Surveiliance			
Clisco Virtual Service Gatewaymerchant / serviceClisco Tirewall Service Gatewayservice, as part of secureClisco Resonanceprovider, as part of secureClisco 1941Wconfiguration standardClisco 2921standardClisco 3945clisco 3945Clisco 7206clisco 3945Clisco 7206clisco 3945Clisco Ass 1002clisco Nexus 7010clisco Nexus 7010Clisco Nexus 5020clisco Security Manager (CSM)HyTrust Applianceclisco WCS ManagerAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAlR-CAP3502iAllentication ManagerRSA Data Protection ManagerRSA authentication ManagerRSA Data Protection ManagerClisco Ula Fervices EngineClisco Ula Express on Services Readyclisco Ula Clisco Secure Access Control ServerClisco Ula Cliped Computing System (UCS)clisco Vice Access Control ServerClisco Vice Access Control Serverclisco Vice Access Control Server			
Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 29251 Cisco 2945 Cisco outers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 AIR-CAP3502 Cisco Identity Services Engine Cisco VIS Express on Services Ready Figline Cisco UUS Express on Services Ready Figline Cisco UUS Express on Services Ready Cisco Vide Surveiliance			
Cisco routers-store Cisco 891W Cisco 891W Cisco 2921 Cisco 2921 Cisco 29251 Cisco 3945 Cisco 3945 Cisco 7006 Cisco 7007 Cisco 70			
Cisco 891W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2951 Cisco 2955 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MSN 5torage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CAT508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3021 AIR-CAP3021 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 Cisco Identity Services Engine Cisco Identity Services Engine Cisco Unified Wireless AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 Cisco Identity Services Engine Cisco Identity Services Engine Cisco Unified Computing System (UCS) Cisco Catalyst Gatway Cisco UCS Express on Services Ready Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco 3945 Cisco 7206 Cisco 7206 Cisco 7206 Cisco Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 9498 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Wick Smager AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 AIR-CAP3020 Cisco Identity Services Engine Cisco Uritual Service Gateway Cisco Cisco Identity Services Engine Cisco Uritual Service Gateway Cisco			part of secure
Cisco 2921 standard Cisco 2951 processes. Cisco 2951 cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco ASR 1002 cisco Science Cisco MDS Storage Switches cisco Science Cisco Catalyst 6509 cisco Catalyst 6509 Cisco Catalyst 6509 cisco Nexus 7010 Cisco Nexus 5020 cisco Security Manager (CSM) HyTrust Appliance cisco Unified Wireless AIR-CT5508 MSE3500 Cisco WCS Manager cisco WCS Manager AIR-CAP3502I AIR-CAP3502I AIR-CAP3502I AIR-CAP3502I AIR-CAP3502I AIR-LAP1262N EMC CLARION Configuration Manager EMC CLARION Configuration Cisco UCS Express on Services Ready Cisco Urtual Service Stengine cisco UCS Express on Services Ready Cisco Urtual Service Stengine cisco UCS Express on Services Ready Cisco Urtual Service Stengine cisco Unified Compunications Manager Cisco Urtual Service Stengine Cisco Urtual Service Stengine cisco UCS Express on Services Ready Cisco Uritied Compunitig Systend UCS) cisco Urtie Server <td></td> <td></td> <td>5</td>			5
Cisco 2951 Cisco 3945 Cisco oruters-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 57010 Cisco Nexus 57010 Cisco Nexus 57020 Cisco Nexus 57020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 Cisco Identity Service Steady Cisco Victual Service Cateway Cisco Victual Service Cateway Cisco Victual Service Cateway Cisco Victual Service Cateway Cisco Victual Service Steady Cisco USS Express on Services Ready Cisco UIS Express on Services Ready Cisco UIS Express on Services Ready Cisco UISS Express Ontrol Server Cisco Victo Surveiliance			
Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP13021 AIR-CAP13021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CA			processes.
Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3			
Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 M5E3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i Cisco Victual Services Engine Cisco Virtual Services Ready Engine Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco 7206 Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Centry Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i Cisco WCS Manager EMC CLARiION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Potierion Manager RSA Authentication Manager RSA Authentication Manager RSA Authentication Manager RSA Data Protection Manager RSA OUSS CICS Express on Services Ready Engine Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP1042N AIR-CAP3502i AIR-CAP3502i AIR-CAP3502E AIR-CAP3502E EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA anthentication Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP35021 AIR-CAP35022 AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA notision Cisco Victual Services Engine Cisco Victual Services Engine Cisco UCS Express on Services Ready Engine Cisco UIS Express on Services Ready Engine Cisco UIFied Communications Manager and IP Phones Cisco Victo Surveillance			
Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP35021 AIR-CAP35022 AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Server Access Control Server Cisco Video Surveillance			
Cisco Nexus 7010 Cisco Nexus 7020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-C75508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP1042N AIR-CAP35021 AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		-	
Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP1042N AIR-CAP3502i AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA aprise Cisco UCS Express on Services Ready Engine Cisco Uritual Service Gateway Cisco UISE Express on Services Ready Engine Cisco Unified Communications Manager and IIP Phones Cisco Unified Communications Manager and IIP Phones Cisco Unified Communications Manager and IIP Phones Cisco Unified Communications		•	
Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1302I AIR-CAP3502I AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco Identity Services Ready Engine Cisco Unified Compunications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
HyTrust Appliance Cisco Unified Computing System (UCS) Cisco Video Surveillance			
Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA antVision Cisco Identity Services Engine Cisco Virtual Services Ready Engine Cisco UCS Express on Services Ready Engine Cisco UICS Express on Services Ready Engine Cisco UICS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones			
Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA antivision Cisco Identity Services Engine Cisco Virtual Services Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Virdeo Surveillance		AIR-CT5508	
AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		MSE3550	
AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARIION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		Cisco WCS Manager	
AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
AIR-LAP1262NEMC Ionix Network Configuration ManagerEMC CLARiiON CX-240RSA Authentication ManagerRSA Data Protection ManagerRSA Data Protection ManagerRSA enVisionCisco Identity Services EngineCisco Virtual Service GatewayCisco UCS Express on Services Ready EngineCisco Unified Communications Manager and IP PhonesCisco Unified Computing System (UCS)Cisco Video Surveillance			
EMC Ionix Network Configuration ManagerEMC CLARIION CX-240RSA Authentication ManagerRSA Authentication ManagerRSA Data Protection ManagerRSA enVisionCisco Identity Services EngineCisco Virtual Service GatewayCisco UCS Express on Services Ready EngineCisco Unified Communications Manager and IP PhonesCisco Unified Computing System (UCS)Cisco Video Surveillance			
Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
RSA Authentication ManagerRSA Data Protection ManagerRSA enVisionCisco Identity Services EngineCisco Virtual Service GatewayCisco UCS Express on Services ReadyEngineCisco Unified CommunicationsManager and IP PhonesCisco Secure Access Control ServerCisco Video Surveillance			
RSA Authentication ManagerRSA Data Protection ManagerRSA enVisionCisco Identity Services EngineCisco Virtual Service GatewayCisco UCS Express on Services ReadyEngineCisco Unified CommunicationsManager and IP PhonesCisco Secure Access Control ServerCisco Video Surveillance			
RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		RSA Data Protection Manager	
Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		RSA enVision	
Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		Cisco Identity Services Engine	
Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance		Cisco Virtual Service Gateway	
Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco Secure Access Control Server Cisco Video Surveillance			
Cisco Video Surveillance			
Cisco Physical Access Control			
		Cisco Physical Access Control	

acce	B.c Verify that administrator ess to the web-based	Verizon Business reviewed non-console administrative access for	Note: Verification of
enci	nagement interfaces is crypted with strong ptography.	all PCI Reference Architecture for Retail Solutions and verified that administrator access to the web-based management interfaces is encrypted with strong cryptography.	telnet presence within the management consoles
		Verizon Business observed system-generated configuration output for the following system components:	(Windows Server 2003) was not performed. This is the
		Cisco ASA 5500 Series-data center	responsibility
		Cisco ASA 5585	of the merchant /
		Cisco ASA 5540	service
		Cisco ASA 5500 Series-store	provider, as
		Cisco ASA 5510	part of secure configuration
		Cisco Virtual Service Gateway	standard
		Cisco Firewall Services Module	processes.
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco Video Surveillance	
providers mustprocprotect eachA.1.entity's hostedAddenvironment andReqcardholder data.HosThese providersassemust meet specificprovrequirements asshaddetailed inprotAppendix A:(meAdditional PCI DSSprov	Perform testing cedures A.1.1 through 4 detailed in Appendix A: ditional PCI DSS quirements for Shared sting Providers for PCI DSS essments of shared hosting widers, to verify that irred hosting providers tect their entities' erchants and service widers) hosted vironment and data.	N/A – For the purpose of this assessment, Cisco is not a hosting provider.	

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
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:			

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).	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.
	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.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.
	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	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.
	does not exceed requirements defined in the data retention policy.	

	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.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.	
 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.	N/A – Cisco is not an Issuer and does not support issuing services.	
	 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 	N/A - It is the responsibility of the merchant to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).	
	authentication data below, perform the following steps:		

	2.3.1 For a second of 1		u	
3.2.1 Do not store the full contents of any track (from the	3.2.1 For a sample of system components, examine data	N/A – It is the responsibility of		
magnetic stripe located on the	sources, including but not limited	the merchant to		
back of a card, equivalent data	to the following, and verify that the	ensure systems		
contained on a chip, or	full contents of any track from the	used do not store		
elsewhere). This data is alternatively called full track,	magnetic stripe on the back of card or equivalent data on a chip are	sensitive authentication		
track, track 1, track 2, and	not stored under any	data (e.g. full		
magnetic-stripe data.	circumstance:	track data, CVV2,		ļ
Note: In the normal course of	Incoming transaction data	PIN/PIN block)		
business, the following data	All logs (for example, transaction,	post authorization		
elements from the magnetic stripe may need to be retained:	history, debugging, error)	(even if		
The cardholder's name	History files	encrypted).		
	Trace files			
Primary account number (PAN)	Several database schemas			
Expiration date	Database contents			
Service code				
To minimize risk, store only				
these data elements as needed				
for business. 3.2.2 Do not store the card	2 2 2 Ear a comple of system	N/A – It is the		
verification code or value	3.2.2 For a sample of system components, examine data	responsibility of		
(three-digit or four-digit number	sources, including but not limited	the merchant to		
printed on the front or back of a	to the following, and verify that the	ensure systems		
payment card) used to verify	three- digit or four-digit card verification code or value printed	used do not store sensitive		
card-not- present transactions.	on the	authentication		
	front of the card or the signature	data (e.g. full		
	panel (CVV2, CVC2, CID, CAV2	track data,		
	data) is not stored under any	CVV2, PIN/PIN block) post		
	circumstance:	authorization		
	Incoming transaction data	(even if		
	All logs (for example, transaction, history, debugging,	encrypted).		
	error)			
	History files			
	Trace files			
	Several database schemas			
	Database contents			ļ
3.2.3 Do not store the personal	3.2.3 For a sample of system	N/A – It is the		
identification number (PIN) or the	components, examine data	responsibility of		
encrypted PIN block.	sources, including but not limited	the merchant to ensure systems		
	to the following and verify that PINs and encrypted PIN blocks are	used do not store		
	not stored under any	sensitive		
	circumstance:	authentication		
	Incoming transaction data	data (e.g. full track data,		
	All logs (for example,	CVV2, PIN/PIN		
	transaction, history, debugging,	block) post		
1	error)			1
	error)	authorization (even if		
	History files	authorization (even if encrypted).		
	History files Trace files	(even if		
	History files	(even if		

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.	N/A – Data control and Data classification policies and procedures, including masking PAN data, except for those with a specific need to see full PAN data, is the responsibility of the merchant.		
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. 	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	N/A - Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider. Verizon Business reviewed RSA Data Protection Manager application, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable RSA Data Protection Manager - 192-bit 3DES or 256-bit AES encryption. RSA Data Protection Manager - 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES	
	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).	encryption. N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.	
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.	
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.	

3.4.1 If disk encryption is used	3.4.1.a If disk encryption is used,	Verizon Business	
(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	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).	reviewed RSA Data Protection Manager, EMC CLARIION CX-240, Cisco MDS Storage Switches, related to protecting sensitive data	
databases). Decryption keys must not be tied to user accounts.		within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable.	
		Note: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these	
		switch, these provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array	
		and Cisco UCS servers in the solution.	
	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).	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. Note : Although	
		the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these	
		systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.	

	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.	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. Note : Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in	
 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	3.5.1 Examine user access lists to	N/A – Protection	 1
cryptographic keys to the fewest	verify that access to keys is	of encryption	
number of custodians necessary.	restricted to the fewest number of	keys is the	
	custodians necessary.	responsibility of the merchant /	
		service provider.	
		Verizon Business	
		confirmed that	
		restricted access	
		to encryption	
		keys is as follows	
		RSA Data Protection	
		Manager: Data	
		encryption keys	
		are never	
		disclosed to the	
		key administrators	
		and cannot be	
		exported to a key	
		administrator.	
		RSA Data	
		Protection Manager security	
		policies require	
		public key	
		authentication to	
		access key	
		material for encryption/decry	
		ption purposes.	
		Verizon Business	
		observed	
		system-generate	
		d configuration	
		output for the	
		following system components:	
		RSA Data	
		Protection	
		Manager	
		Cisco MDS	
		Storage Switches	

3.5.2 Store cryptographic keys	3.5.2.a Examine system	N/A – Protection]
securely in the fewest possible locations and forms.	configuration files to verify that keys are stored in encrypted	of encryption keys is the	
	format and that key-encrypting	responsibility of	
	keys are stored separately from	the merchant /	
	data-encrypting keys.	service provider.	
		RSA Data Protection	
		Manager: Key	
		encryption key is stored in	
		memory and	
		data encryption	
		keys are stored in encrypted	
		format within	
		Oracle or MS SQL database.	
		Verizon Business	
		observed	
		system-generate d configuration	
		output for the	
		following system	
		components:	
		RSA Data Protection	
		Manager	
		Cisco MDS	
	3.5.2.b Identify key storage	Storage Switches N/A – Protection	
	locations to verify that keys are	of encryption	
	stored in the fewest possible	keys is the	
	locations and forms.	responsibility of the merchant /	
		service provider.	
		Verizon Business	
		observed system-generate	
		d configuration	
		output for the	
		following system components:	
		RSA Data	
		Protection Manager	
		Cisco MDS	
		Storage Switches	

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	3.6.a Verify the existence of key-management procedures for keys used for encryption of cardholder data.	N/A – Key Management policy and procedures is the responsibility of the merchant / service provider.	
Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	N/A - Key Management policy and procedures is the responsibility of the merchant / service provider.	
	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.	N/A - Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that generation of strong keys is included for the following: RSA Data Protection Manager: 192-bit 3DES or 128-bit/192-bit/2 56-bit AES keys Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches	

3.6.2 Secure cryptographic key	3.6.2 Verify that key-management	N/A – Key	
distribution	procedures are implemented to	Management	
	require secure key distribution.	policies and	
		procedures is the	
		responsibility of	
		the merchant /	
		service provider.	
		Verizon Business	
		confirmed that	
		secure distribution	
		of keys is included	
		for the following:	
		RSA Data	
		Protection	
		Manager: All key	
		transfers are done over SSLv3/TLSv1	
		connections	
		between Key	
		Manager Server	
		and Key Manager	
		Clients.	
		Verizon Business	
		observed	
		system-generated	
		configuration	
		output for the	
		following system	
		components:	
		RSA Data	
		Protection	
		Manager	
		Cisco MDS	
		Storage Switches	

3.6.3 Secure cryptographic key storage	3.6.3 Verify that key-management procedures are implemented to require secure key storage.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider.	
		Verizon Business confirmed that secure key storage is included for the following:	
		RSA Data Protection Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database.	
		Verizon Business observed system-generated configuration output for the following system components:	
		RSA Data Protection Manager	
		Cisco MDS Storage Switches	

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of	3.6.4 Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.	N/A – Key Management policies and procedures is the	
time has passed and/or after a certain amount of cipher- text has been produced by a given		responsibility of the merchant / service provider.	
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).		Verizon Business confirmed that key rotation capabilities are included for the following:	
		RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined.	
		Verizon Business observed system-generated configuration output for the following system components:	
		RSA Data Protection Manager	
		Cisco MDS Storage Switches	

3.6.5 Retirement or replacement	3.6.5.a Verify that	N/A – Key	
(for example, archiving,	key-management procedures are	Management	
destruction, and/or revocation) of keys as deemed necessary when	implemented to require the retirement of keys when the	policies and procedures is the	
the integrity of the key has been	integrity of the key has been	responsibility of	
weakened (for example,	weakened.	the merchant /	
departure of an employee with		service provider.	
knowledge of a clear-text key), or		Verizon Business	
keys are suspected of being compromised.		confirmed that	
compromised.		destruction of keys is included	
		for the following:	
Note: If retired or replaced cryptographic keys need to be		RSA Data	
retained, these keys must be		Protection	
securely archived (for example,		Manager: RSA	
by using a key encryption key).		Data Protection	
Archived cryptographic keys		Manager assigns	
should only be used for decryption/verification purposes.		lifetimes for key use, and policies	
deci yption/vermeation purposes.		can be created to	
		rotate (generate	
		and use new	
		key) as	
		frequently as defined, or	
		delete, when	
		necessary.	
	3.6.5.b Verify that the	N/A – Key	
	key-management procedures are implemented to require the	Management policies and	
	replacement of known or	procedures is the	
	suspected compromised keys.	responsibility of	
		the merchant /	
		service provider.	
		Verizon Business confirmed that	
		replacement of	
		known or	
		suspected	
		compromised	
		keys is included for the following:	
		RSA Data	
		Protection	
		Manager: RSA	
		Data Protection	
		Manager assigns lifetimes for key	
		use, and policies	
		can be created to	
		rotate (generate	
		and use new	
		key) as frequently as	
		defined	

3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.			
for encryption operations. procedures is the procedures is the proc	cryptographic keys are retained,		
responsibility of the merchant / service provider. Verizon Business confirmed that retired or replaced cryptographic keys are netained, and that these keys are not used for encryption opperations for operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection			
the merchant / service provider. Verizon Business confirmed that retired or replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager and mager cisco MDS	for encryption operations.		
service provider. Verizon Business confirmed that retired or replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protections Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed observed configuration output for the following system components: RSA Data Protection Based of the system components: RSA Data Protection Based of the system components: RSA Data Protection Based of the system components: RSA Data Protection Manager Clisco MDS			
Verizon Business confirmed that retired or replaced Cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed defined Verizon Business observed configuration output for the following system components: RSA Data Protection Manager RSA Data			
confirmed that retired or replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection			
cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager			
keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
operations for the following: RSA Data Protection Manager: RSA Data Protection Manager asigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager			
the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager			
RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS		-	
Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS		Data Protection	
use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
frequently as definedVerizon Business observedobservedsystem-generated configuration output for the following system components:RSA Data Protection ManagerCisco MDS		and use new	
defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
configuration output for the following system components: RSA Data Protection Manager Cisco MDS			
following system components: RSA Data Protection Manager Cisco MDS		configuration	
components: RSA Data Protection Manager Cisco MDS			
RSA Data Protection Manager Cisco MDS			
Protection Manager Cisco MDS			
Manager Cisco MDS			
Cisco MDS			
		Cisco MDS	

3.6.6 If manual clear-text	3.6.6 Verify that manual clear-text	N/A – Key	
cryptographic key management	key-management procedures	Management	
operations are used, these operations must be managed	require split knowledge and dual control of keys.	policies and procedures is the	
using split knowledge and dual	control of keys.	responsibility of	
control (for example, requiring		the merchant /	
two or three people, each		service provider.	
knowing only their own key		Verizon Business	
component, to reconstruct the		confirmed that	
whole key).		split	
		knowledge/dual	
Note: Examples of manual key		control of keys is included for the	
management operations include,		following:	
but are not limited to: key		5	
generation, transmission, loading, storage and destruction.		RSA Data Protection	
loading, storage and destruction.		Manager: Data	
		encryption keys	
		are never	
		disclosed to the	
		key	
		administrators and cannot be	
		exported at any	
		time in clear-text	
		format.	

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.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider.	
		Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following:	
		RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. Key administration	
		functions can only be access through the Key Manager server, via access controls (authentication) through the RSA Access Manager server.	
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.	N/A – Key custodian lists are the responsibility of the merchant/service provider.	

Requirement 4: Encrypt transmission of cardholder data across open, public networks

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
----------------------	--------------------	----------	--------------	----------

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, EC, 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:	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that it uses security protocols wherever cardholder data is transmitted or received over open, public networks. Note: Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco Firewall Services Module Cisco routers-store Cisco S91W Cisco 1941W Cisco 2921 Cisco 3945 Cisco ASR 1002 Cisco 7206 Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i	
		AIR-CAP3502E AIR-LAP1262N	
	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.	Note: Verizon Business reviewed wireless settings within the PCI Solution for Retail environment to confirm WPA encryption has been implemented for all wireless traffic.	
	4.1.b Verify that only trusted keys and/or certificates are accepted.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that 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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.	
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that the proper encryption strength is implemented for the encryption methodology in use.	
	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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that for SSL/TLS implementations, HTTPS appears as a part of the browser 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.	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.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment to confirm that WPA encryption has been implemented for all wireless traffic.	
Note: The use of WEP as a security control was prohibited as of 30 June 2010.		observed system-generated configuration output for the following system components: Cisco Unified Wireless	
		AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N	

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.	N/A – Data Control / Encryption policy and procedures is the responsibility of the merchant / service provider.	
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	N/A – Data Control / Encryption policy and procedures is the responsibility of the merchant / service provider.	

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business- approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
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.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		
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).	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	 5.2 Verify that all anti-virus software is current, actively running, and generating 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. 	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider. N/A – Written A/V policy is the responsibility of the merchant / service provider.	
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.	
	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.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.	
	5.2.d For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7	N/A – Central storage and retention of A/V logs is the responsibility of the merchant / service provider.	

Requirement 6: Develop and maintain secure systems and applications

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

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

PCI DSS Requirements Testing Procedures In Place Not In Place Comments

Γ

6.1 Ensure that all system	6.1.a For a	Verizon Business reviewed		
components and software are	sample of system	configurations for the PCI		
protected from known	components and	Reference Architecture for Retail Solution components,		
vulnerabilities by having the	related software,	including management		
latest vendor-supplied security	compare the list	consoles for components		
patches installed. Install critical	of security	within the PCI Solution for		
security patches within one	patches installed	Retail environment and confirmed they are running		
month of release.	on each system to	current software releases and		
	the most recent	contain current vendor		
Note: An organization may		patches as of the time of this		
consider applying a risk-based	vendor security	assessment.		
approach to prioritize their patch	patch list, to	Verizon Business observed system-generated		
installations. For example, by	verify that current	configuration output for the		
prioritizing critical infrastructure	vendor patches	following system components:		
(for example, public-facing	are installed.	Cisco ASA 5500 Series-data		
devices and systems,		center		
databases) higher than		Cisco ASA 5585		
less-critical internal devices, to		Cisco ASA 5540		
ensure high-priority systems		Cisco ASA 5500 Series-store		
and devices are addressed		Cisco ASA 5510		
within one month, and		Cisco Virtual Service Gateway		
addressing less critical devices		Cisco Firewall Services Module		
and systems within three		Cisco routers-store		
months.		Cisco 891W		
monuns.		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager (CSM)		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network		
		Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on		
		Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System (UCS)		
		Cisco Secure Access Control		
		Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
		,	I	1

	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.	N/A – Patch management policy and procedures is the responsibility of the merchant / service provider.	
 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 	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	N/A – Patch / Risk management policy and procedures is the responsibility of the merchant / service provider.	
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.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.	N/A – Patch / Risk management policy and procedures is the responsibility of the merchant / service provider. Verizon Business recommends using multiple outside sources (e.g. SANS, CERT, SecurityFocus, vendor websites, etc) to identify new vulnerability issues within the environment.	

6.3 Develop software applications (internal and external, and including web- based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	 6.3.a Obtain and examine written software development processes to verify that the processes are based on industry standards and/or 6.3.b Examine written software development processes to verify that information security is included throughout the life cycle. 	N/A – Software Development was not in scope for this assessment. N/A – Software Development was not in scope for this assessment.	
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with 6.3.d From an examination of	N/A – Software Development was not in scope for this assessment.	
	written software development processes, and interviews of software developers, verify		
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	N/A – Software Development was not in scope for this assessment.	

6.3.2 Review of custom code	6.3.2.a Obtain	N/A – Software	
prior to release to production or	and review	Development was not in	
customers in order to identify	policies to confirm	scope for this assessment.	
any potential coding	that all custom		
vulnerability.	application code		
	changes must be		
	reviewed (using		
Note: This requirement for code	either manual or		
reviews applies to all custom	automated		
code	processes) as		
(both internal and	follows:		
public-facing), as part of the	Code changes		
system development life cycle.	are reviewed by		
Code reviews can be conducted	individuals other		
by knowledgeable internal	than the		
personnel or third parties. Web	originating code		
applications are also subject to	author, and by		
additional controls, if they are	individuals who		
public facing, to address	are		
ongoing threats and	knowledgeable in		
vulnerabilities after	code review		
implementation, as defined at	techniques and		
PCI DSS Requirement 6.6.	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.		
	6.3.2.b Select a	N/A – Software	
	sample of recent	Development was not in	
	custom	scope for this assessment.	
	application		
	changes and		
	verify that custom		
	application code is		
	reviewed		
	according to		
	6.3.2.a, above.		

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	6.4 From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:		
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.	N/A – Software Development was not in scope for this assessment.	
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.	N/A – Software Development was not in scope for this assessment.	
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.	N/A – Software Development was not in scope for this assessment.	
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.	N/A – Software Development was not in scope for this assessment.	

6.4.5 Change control	6.4.5.a Verify	N/A – Software	
procedures for the	that	Development was not in	
implementation of security	change-control	scope for this assessment.	
patches and software	procedures		
modifications. Procedures	related to		
must include the following:	implementing security patches		
	and software		
	modifications are		
	documented and		
	require items		
	6.4.5.1 - 6.4.5.4		
	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		
6.4.5.1 Documentation of	6.4.5.1 Verify	N/A – Security	
impact.	that	Policy/Procedures	
	documentation of	(Change Control) is the	
	impact is included	responsibility of the	
	in the change	merchant / service	
	control	provider.	
	documentation for		
	each sampled		
	change.		
6.4.5.2 Documented change	6.4.5.2 Verify	N/A – Security	
approval by authorized parties.	that documented	Policy/Procedures	
	approval by authorized parties	(Change Control) is the responsibility of the	
	is present for each	merchant / service	
	sampled change.	provider.	
	Sampica change.		
	1		

6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	 6.4.5.3.a For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. 6.4.5.3.b For custom code changes, verify that all updates are tested for 	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider. N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service	
6.4.5.4 Back-out procedures.	compliance with PCI DSS Requirement 6.5 before being deployed into production. 6.4.5.4 Verify	provider. N/A – Security	
	that back-out procedures are prepared for each sampled change.	Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.	
 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 	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	N/A – Software Development is not in scope for assessment.	
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	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in	N/A – Software Development is not in scope for assessment.	
Coding, etc.), the current best practices must be used for these requirements.	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:		

6.5.1 Injection flaws,	C E 4 Turis shiers			
	6.5.1 Injection	N/A – Software		
particularly SQL injection. Also	flaws, particularly	Development is not in		
consider OS Command	SQL injection.	scope for assessment.		
Injection, LDAP and XPath	(Validate input to			
injection flaws as well as other	verify user data			
injection flaws.	cannot modify			
	meaning of			
	commands and			
	queries, utilize			
	parameterized			
6.5.2 Buffer overflow	queries, etc.) 6.5.2 Buffer	N/A – Software		
0.3.2 Duffer overflow				
	overflow (Validate	Development is not in		
	buffer boundaries	scope for assessment.		
	and truncate input			
	strings.)			
	5,			
6.5.3 Insecure cryptographic	6.5.3 Insecure	N/A – Software		
storage	cryptographic	Development is not in		
storage				
	storage (Prevent	scope for assessment.		
	cryptographic			
	flaws)			
6.5.4 Insecure communications	6.5.4 Insecure	N/A – Software	+	
0.3.4 Insecure communications				
	communications	Development is not in		
	(Properly encrypt	scope for assessment.		
	all authenticated			
	and sensitive			
	communications)			
	communications)			
6.5.5 Improper error handling	6.5.5 Improper	N/A – Software		
	error handling (Do	Development is not in		
	not leak	scope for assessment.		
	information via			
	error messages)			
	- /			
6.5.6 All "High" vulnerabilities	6.5.6 All "High"	N/A – Software		
identified in the vulnerability	vulnerabilities as	Development is not in		
identification process (as	identified in PCI	scope for assessment.		
defined in PCI DSS Requirement	DSS Requirement			
	6.2.			
6.2).	0.2.			
Note: Requirements 6.5.7				
through				
6.5.9, below, apply to web				
applications and application				
interfaces (internal or external):				
6.5.7 Cross-site scripting (XSS)	6.5.7 Cross-site	N/A – Software		
,				
		scope for assessment.		
	escaping, etc.)			
6.5.7 Cross-site scripting (XSS)	scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive	N/A – Software Development is not in scope for assessment.		

r	r		1	
6.5.8 Improper Access Control	6.5.8 Improper	N/A – Software		
(such as insecure direct object	Access Control,	Development is not in		
references, failure to restrict	such as insecure	scope for assessment.		
URL access, and directory	direct object			
traversal)	references, failure			
,	to restrict URL			
	access, and			
	directory traversal			
	(Properly			
	authenticate users			
	and sanitize input.			
	•			
	Do not expose			
	internal object			
6.5.9 Cross-site request forgery	6.5.9 Cross-site	N/A – Software		
(CSRF)	request forgery	Development is not in		
	(CSRF). (Do not	scope for assessment.		
	reply on			
	authorization			
	credentials and			
	tokens			
	automatically			
L	automatically			
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------	------	
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	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	N/A – Public-facing web applications are not in scope for assessment.		
vulnerability security assessment tools or methods, at least annually and after any changes Installing a web-application	either manual or automated vulnerability security assessment tools or methods), as follows:			
firewall in front of public-facing web	- At least annually			
applications	 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.			

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

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

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
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	7.1.1 Confirm that access	Verizon Business confirmed	
rights to privileged user	rights for privileged user IDs	privileged user IDs are restricted to the least	
IDs to least privileges	are restricted to least	privileges necessary to	
necessary to perform job	privileges necessary to	perform job functions and	
responsibilities	perform job responsibilities.	exist for the following components.	
		•	
		Verizon Business observed system-generated	
		configuration output for the	
		following system	
		components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services	
		Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager RSA Data Protection Manager	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services	
		Engine	
		Cisco Virtual Service Gateway	
		-	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		and IP Phones	
		Cisco Unified Computing System (UCS)	
		System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
		Cisco i mysical Access Control	

7.1.2 Assignment of 7.1.2 Confirm that	
privileges is based on are assigned to ind	
individual personnel's job based on job classif	following components.
classification and function function (also calle	
"role-based access	control" or system-generated
RBAC).	configuration output for the following system
	components:
	Cisco ASA 5500 Series-data
	center
	Cisco ASA 5585
	Cisco ASA 5540
	Cisco ASA 5500 Series-store
	Cisco ASA 5510
	Cisco Virtual Service Gateway
	Cisco Firewall Services Module
	Cisco routers-store
	Cisco 891W
	Cisco 1941W
	Cisco 2921
	Cisco 2951
	Cisco 3945
	Cisco routers-data center
	Cisco ASR 1002
	Cisco 7206
	Cisco MDS Storage Switches
	Cisco switches-data center
	Cisco Catalyst 6509
	Cisco Catalyst 4948
	Cisco Nexus 7010
	Cisco Nexus 5020
	Cisco Security Manager (CSM)
	HyTrust Appliance
	Cisco Unified Wireless
	AIR-CT5508
	MSE3550
	Cisco WCS Manager
	AIR-CAP1042N
	AIR-CAP3502i
	AIR-CAP3502E
	EMC Ionix Network Configuration Manager
	EMC CLARION CX-240
	RSA Authentication Manager
	5
	RSA Data Protection Manager
	RSA enVision
	Cisco Identity Services Engine
	Cisco Virtual Service Gateway
	Cisco UCS Express on Services Ready Engine
	Cisco Unified Communications Manager
	Communications Manager and IP Phones
	Cisco Unified Computing
	System (UCS)
	Cisco Secure Access Control
	Server
	Cisco Video Surveillance
	Cisco Physical Access Control

documented approval by specifying required privileges.	7.1.3 Requirement for a	7.1.3 Confirm that	Verizon Business observed	
specifying required in writing or electronically) for all access, and that it must specify required privileges. If the specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges is a specify required privileges. If the specify required privileges is a specify required privileges is a specify required privileges is a specify required privileges. If the specify required privileges is a specify required privilege is a specify required privileges is a specify required privilege is a specify re	authorized parties	authorized parties is required	configuration output for the following system	
Circo ASA 5583 Circo ASA 5500 Circo ASA 5500 Circo ASA 5500 Circo ASA 5500 Circo ASA 5500 Circo Circo ASA 500 Circo Circo Circo ASA 1002 Circo 7206 Circo Circo ASA 1002 Circo Circo Circo Asa Control Circo Circo Circo Asa Circo Circ		for all access, and that it must	Cisco ASA 5500 Series-data	
Cisco ASA 5540 Cisco ASA 5500 Serie-store Cisco ASA 5510 Cisco Virtual Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2951 Cisco 7041W Cisco 2951 Cisco 7040 Cisco 7046 Cisco routers-data center Cisco ASR 1002 Cisco 7026 Cisco MDS Storage Switches Cisco routers-data center Cisco Catalyst 6509 Cisco Catalyst 6500 Cisco Catalyst 7000 Cisco Catalyst 70000 Cisco Catalyst		specify required privileges.		
Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco R91W Cisco 1941W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 2921 Cisco 2945 Cisco 7206 Cisco R002 Cisco 7206 Cisco ASR 1002 Cisco 7206 Cisco ASR 1002 Cisco Catalyst 4948 Cisco ASR 4948 Cisco ASR 4948 Cisco Asevas 5020 Cisco Catalyst 4948 Cisco Asevas 5020 Cisco Catalyst 4948 Cisco Asevas 5020 Cisco Catalyst 4948 Cisco Asevas 5020 Cisco Catalyst 4948 Cisco Mexus 5020 Cisco Mexus 5020 Cisco Catalyst 4948 Cisco Mexus 5020 Cisco Mexus 5020 Cisco Mined Mineless AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 Cisco Mick Metwork Configuration Manager RSA Authentication Manager RSA Authentication Manager RSA Authentication Manager RSA envision Cisco Virtual Services Engine Cisco Virtual Services Son Manager and IP Phones Manager Cisco Virtual Services Control Services Secure Access Control Services Manager Cisco Virtual Services Sinter (UCS) Cisco Mifeed Computing System (UCS)				
Cisco XAS 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 2951 Cisco 3945 Cisco 3945 Cisco ASR 1002 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco WCS Manager AIR-CAP3502I AUBR-CAR35 Authenticiat				
Cisco Frewall Services Module Cisco routers-store Cisco 991W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Sutches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 7020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE5350 Cisco WCS Manager AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 Cisco Manager RSA Authentication Manager RSA Authentication Manager RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco UCS Express on Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server				
Module Cisco Touters-store Cisco 891W Cisco 2921 Cisco 2951 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Security Manager (CSW) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i EMC Lonxi Network EMC Lonxi Network EMC Lonxi Network EMC Lonxi Network EMC Lonxi Network EMC Lonxi Network Configure on Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Uritual Services Engine Cisco Uritual Services Cateway Cisco Uritual Services Ready Engine Cisco Uritual Services Cateway Cisco Uritual Services Ready Engine Cisco Uritual Services Cateway Cisco Uritual Services Cisco Uritual Services Ready Engine Cisco Uritual Services Cateway Cisco Uritual Services Ready Engine Cisco Uritual Services Control Server Cisco Uritual Service Cortrol Server			Cisco Virtual Service Gateway	
Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 2945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MSD Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CA75508 MSE3550 Cisco WCS Manager AIR-CA75021 AIR-CA735021 Cisco WCS Manager RSA Authentication Manager RSA Data Protection Manager RSA Authentication Manager RSA Data Protection Manager RSA Cathentication Manager Cisco Virtual Service Cateway Cisco Unified Computing System (UCS) Cisco Server Jones Cisco Server Access Control Server Cisco Server Access Control Server			Cisco Firewall Services Module	
Cisco 1941W Cisco 2921 Cisco 2951 Cisco 2951 Cisco 7945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco MDS Storage Switches Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Souro Cisco Security Manager Cisco Mexus 5020 Cisco Security Manager Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i Cisco Infiguration Manager RSA Data Protection Manager RSA Authentication Manager RSA Protection Manager RSA ent/Sion Cisco Victal Service Gateway Cisco Victal Service Gateway Cisco Victal Service Gateway Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Unified Computing System (UCS)			Cisco routers-store	
Cisco 2921 Cisco 2951 Cisco 2945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MSD Storage Switches Cisco catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 57010 Cisco Nexus 57010 Cisco Nexus 57010 Cisco Nexus 57010 Cisco Security Manager Cisco Societa Virust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i Cisco Titual Service Sateway Cisco Titual Service Sateway Cisco Virtual Service Gateway Cisco Virtual Service Gateway Cisco Unified Cisco Unified Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Virtual Ince			Cisco 891W	
Cisco 2951 Cisco 3945 Cisco 7206 Cisco ASR 1002 Cisco 7206 Cisco 7206 Cisco Tables Galacterer Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 Cisco Tables Manager RSA Authentication Manager RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager Cisco UICS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Server Access Control Server			Cisco 1941W	
Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Storage Switches Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 AIR-CAP35021 Cisco Nexus Manager EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Virtual Services Engine Cisco Virtual Services Gateway Cisco Unified Communications Manager and Phones Cisco Unified Computing System (UCS) Cisco Server Access Control Server				
Cisco routers-data center Cisco ASR 1002 Cisco Z206 Cisco 7206 Cisco MDS Storage Switches Cisco atalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager Cisco Security Manager Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP35021 AIR-CAP35021 AIR-CAP3502E EMC Ionix Network Configuration Manager RSA Data Protection Manager RSA ent/ision Cisco Unified Services Engine Cisco Unitied Services Engine Cisco Unitied Services Cisco Unitied Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Services Control Service Server Cisco Virtual Services Cateway Cisco Unified Computing System (UCS) Cisco Secure Access Control Services Cateway Cisco Virtual Services Cateway Cisco Unified Computing System (UCS) Cisco Secure Access Control				
Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Aptilance Cisco Unified Wireless AIR-CTS508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i EMC Clonki Network Configuration Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Virtual Services Engine Cisco Virtual Services Engine Cisco Virtual Services Engine Cisco Virtual Services Cisco Unified Cisco Unified Cisco Unified Computing System (UCS)				
Cisco MDS Storage Switches Cisco Switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP3502E EMC LORIX Network Configuration Manager EMC CLARIION CX-240 RSA Data Protection Manager RSA Data Protection Manager RSA Data Protection Manager Cisco UCS Express on Services Ready Engine Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
Cisco switches-diata center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARIION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Uitual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Compunications Manager and IP Phones Cisco Unified Compunications Manager Cisco Uitual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Compunications Manager Cisco Unified Compunications Manager Cisco Unified Computing System (UCS) Cisco Secure Access Control Server			Cisco 7206	
Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Clonix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA pata Protection Manager RSA enVision Cisco Uritual Services Engine Cisco Uritual Services and Engine Cisco Uritual Service Gateway Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager Cisco Video Surveillance			Cisco MDS Storage Switches	
Cisco Catalyst 4948 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP1042N AIR-CAP3502i AIR-CAP3502i AIR-CAP3502E EMC Lonix Network Configuration Manager EMC CLARIION CX-240 RSA Authentication Manager RSA authentication Manager RSA authentication Manager Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Ready Engine Cisco Unified Communications Manager and IP Phoness Cisco Unified Computing System (UCS) Cisco Secure Access Control Server			Cisco switches-data center	
Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP3502i AIR-CAP3502i AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Virtual Services Engine Cisco Virtual Service Gateway Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones			Cisco Catalyst 6509	
Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARIION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Potention Manager Cisco Virtual Services Engine Cisco Virtual Service Gateway Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Viceo Surveillance			-	
Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP35021 AIR-CAP3502E EMC Lonix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA anthentity Services Engine Cisco Ufrual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Server				
(CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502i AIR-CAP3502E EMC Lonix, Network Configuration Manager EMC CLARION CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco Virtual Services Ready Engine Cisco Virtual Services Ready Engine Cisco Virtual Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server				
Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA activities Engine Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco Urital Service Gateway Cisco Urital Service Gateway Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance			Cisco Security Manager (CSM)	
AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA Data Protection Manager Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco Virtual Services Seady Engine Cisco Unified Communications Manager and IP Phones Cisco Secure Access Control Server Cisco Video Surveillance				
MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Uirtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server				
Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server				
AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Virteo Surveillance				
AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server			5	
AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones Cisco Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Secure Access Control Server Cisco Video Surveillance				
RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			_	
Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			_	
Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			Engine	
Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			-	
Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance			Cisco UCS Express on Services Ready Engine	
Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance				
Cisco Secure Access Control Server Cisco Video Surveillance				
Cisco Video Surveillance			Cisco Secure Access Control	
Cisco Physical Access Control				
cisco invisical Access Control			Cisco Physical Access Control	

			1
7.1.4 Implementation of an automated access control system	7.1.4 Confirm that access controls are implemented via an automated access control	Verizon Business confirmed automated access controls exist for the following	
control system	system.	components.	
	system.	Verizon Business observed	
		system-generated configuration output for the	
		following system	
		components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W Cisco 2921	
		Cisco 2921 Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		SSL VPN	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

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 all" unless specifically allowed.	7.2 Examine system settings and vendor documentation to verify that an access control system is implemented as follows:		
This access control system must include the following:			

			,
7.2.1 Coverage of all	7.2.1 Confirm that access	Verizon Business reviewed	
system components	control systems are in place	system components and verified that access control	
	on all system components.	systems are in place on all	
		PCI Reference Architecture	
		for Retail Solutions components.	
		Verizon Business observed	
		system-generated	
		configuration output for the	
		following system components:	
		Cisco ASA 5500 Series-data	
		center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services	
		Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951 Cisco 2045	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010 Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services	
		Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
		,	

7.2.2 Assignment of	7.2.2 Confirm that access	Verizon Business reviewed	
privileges to individuals	control systems are configured	system components and verified that access control	
based on job classification	to enforce privileges assigned	systems include role-based	
and function	to individuals based on job	privilege assignment for all PCI Reference Architecture	
	classification and function.	for Retail Solutions	
		components.	
		Verizon Business observed	
		system-generated	
		configuration output for the following system	
		components:	
		Cisco ASA 5500 Series-data	
		center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services	
		Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARiiON CX-240	
		RSA Authentication Manager	
		5	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services	
		Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
		Cisco i nysical Access Control	

7.2.3 Default "deny-all" setting	7.2.3 Confirm that the access control systems have a default	Verizon Business reviewed system components and	
setting	· ·	verified that access control	
	"deny-all" setting.	systems include default "deny-all" settings on all PCI Reference Architecture for	
Note: Some access control		Reference Architecture for Retail Solutions components.	
systems are set by default to "allow-all," thereby		Verizon Business observed	
permitting access		system-generated	
unless/until a rule is		configuration output for the following system	
written to specifically deny		components:	
it.		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945 Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010 Cisco Nexus 502	
		<u>Cisco</u> Security Manager	
		(CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

Requirement 8: Assign a unique ID to each person with computer access

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

Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

PCI DSS Requirements Testing Procedures In Place Not in Place Comme	
---------------------------------------------------------------------	--

Γ

 8.1 Sasign all users a unique ID for access to system components or cardholder data. 8.1 Vertion Business reviewed access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components or cardholder data. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.1 Sasign all users a unique ID for access to system components. 9.2 Sasign all users a unique ID for access to system components. 9.3 Sasign all users a unique ID for access to system components. 9.4 Sasign all users a unique ID for access to the component of the system component to the following system c				1	1
	ID before allowing them to access system components	users are assigned a unique ID for access to system components or	access lists on all PCI Reference Architecture for Retail Solution components and verified that all users are assigned a unique ID for access to system components or cardholder data. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-data Center Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco ASR 1002 Cisco ASR 1002 Cisco XITUR Services Cisco Switches-data center Cisco ASR 1002 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA Data Protection Manager RSA EnVision Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Unified Computing System (UCS) Cisco Virtual Services Engine Cisco Unified Computing System (UCS)		

· · · · · · · · · · · · · · · · · · ·		l	
 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).	Verizon Business reviewed authentication methods, including observation of live login attempts and verified that a unique ID and password was required for each authentication attempt to all PCI Reference Architecture for Retail Solution components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-data center Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Services Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco ASR 1002 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP35021 AIR-CAP35021 AIR-CAP35022 EMC Lonix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA enVision Cisco Identity Services Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Communications Manager and IP Phones	
		Cisco Secure Access Control Server Cisco Video Surveillance	
		Cisco Video Surveillance Cisco Physical Access Control	

 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. Note: Two-factor authentication. Note: Two-factor 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. 	Verizon Business reviewed these components and verified that two-factor authentication was used for remote access. Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 RSA Authentication Manager with SecurID Note : All products that can use RADIUS authentication would be able to use the two-factor authentication capabilities of RSA Authentication Manager with SecurID.		Two-factor authenticatio n for all remote access, including for employees, contractors, and third parties, is the responsibility of the merchant / service provider.
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	1		,
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	Verizon Business reviewed configuration settings of all PCI Reference Architecture for Retail Solution components and verified that passwords are unreadable during transmission and storage.	
	transmission and storage.	Verizon Business observed system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM) HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System	
		(UCS) Cisco Secure Access Control	
		Server	
		Cisco Video Surveillance Cisco Physical Access Control	
		CISCO FITYSICAL ACCESS CONTON	

	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.	N/A – For the purpose of this assessment, Cisco is not a service provider.	
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 form to the system. 	 N/A - Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Creation of access request (authorization) forms for access to PCI "in scope" systems, including: firewalls, routers, switches, VPNs, AD domain access, servers, databases, and applications, is the responsibility of the merchant / service provider. 	
8.5.2 Verify user identity before performing password resets.	8.5.2 Examine password/authenticati on 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.	 N/A - Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Account management / password reset procedures are the responsibility of the merchant / service provider. 	

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.	 N/A - Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Account management / password reset procedures are the responsibility of the merchant / service provider. 	
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.	N/A – Processes to ensure prompt revocation of granted access rights and deletion / disabling of user IDs is the responsibility of the merchant / service provider.	

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.	N/A - No external vendor accounts were identified during the assessment.	
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.	N/A – No external vendor accounts were identified during the assessment.	
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.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.	

 9.5.3 Do not use group, authentication methods. 9.5.3.6 For a sample of system components, examine components, examine components, examine components are disabled or removed 9.5.6.1 Generic user ID is to verify the following: 9.5.6.1 Generic user ID is to verify the following: 9.5.6.1 Generic user ID is to verify the following: 9.5.6.2 Generic user ID is to verify the following: 9.5.6.2 Generic user ID is to verify the following: 9.5.6.2 Generic user ID is to verify the following: 9.5.6.2 Generic user ID is the verify the following: 9.5.6.2 Generic user ID is and accounts are disabled or removed 9.5.6.2 Generic user ID is an other context functions do inclusion is solved and generic or the exist 5.5.7 Shared and generic Cisco ASA 5550 1.5.6.2 Generic user ID is an other context functions do inclusion is solved and generic context functions do inclusion is solved and generic Cisco ASA 5510 1.5.6.2 Cisco ASA 5510 1.5.6.2 Cisco Firewall Services Module 1.5.6.2 Cisco ASA 5500 1.5.6.2 Cisco ASA 5500 1.5.6.2 Cisco ASA 5500 1.5.6.2 Cisco ASA 5500 1.5.6.2 Cisco ASA 5510 1.5.6.2 Cisco ASA 5510			Γ	
	shared, or generic accounts and passwords, or other	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	ID lists for all PCI Reference Architecture for Retail Solution components and verified that generic or shared user IDs and accounts are not used. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5540 Cisco ASA 5540 Cisco ASA 5510 Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 1941W Cisco 2921 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco ASR 1002 Cisco ASR 1002 Cisco Catalyst 6509 Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco WCS Manager AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA enVision Cisco USE Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control	
			Server	
I Cisco Physical Access Control			Cisco Physical Access Control	

8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	N/A – Security Policy (Password policy/procedures) is the responsibility of the merchant / service provider.	
8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.	N/A – Security Policy (Password policy/procedures) is the responsibility of the merchant / service provider.	

8.5.9 Change user	8.5.9.a For a sample	Verizon Business reviewed	UCS-SRE
passwords at least every 90	of system	configuration settings for	may require
days.	components, obtain	authentication methods to verify that all PCI Reference	compensating
	and inspect system	Architecture for Retail Solutions	controls.
	configuration settings	are configured to change user passwords at least every 90	For routers,
	to verify that user	days.	switches,
	password parameters are set to require	Verizon Business observed	firewalls, you
	users to change	system-generated configuration output for the following system	will need
	passwords at least	components:	manual
	every 90 days.	Cisco ASA 5500 Series-data center	reviews to accomplish,
		Cisco ASA 5585	or use an
		Cisco ASA 5540	external AAA service such
		Cisco ASA 5500 Series-store	as TACACS or
		Cisco ASA 5510	RADIUS
		Cisco Virtual Service Gateway	which can
		Cisco Firewall Services Module	perform this
		Cisco routers-store	function for
		Cisco 891W	user
		Cisco 1941W	accounts.
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server Cisco Video Surveillance	
		Cisco Physical Access Control	

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.	service provider.		
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------	--	--

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	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to require a minimum password length of at least seven characters.		UCS-SRE may require compensating controls
	password parameters are set to require passwords to be at least seven characters	Verizon Business observed system-generated configuration output for the following system components:		
	long.	Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921 Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager (CSM)		
		HyTrust Appliance Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E EMC Ionix Network Configuration		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System (UCS)		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
	1		l	

8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements.	N/A – For the purpose of this assessment, Cisco is not a service provider.		
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------	--	--

8.5.11 Use passwords	8.5.11.a For a	Verizon Business reviewed	UCS-SRE
containing both numeric and alphabetic characters.	sample of system components, obtain and inspect system configuration settings	configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to use passwords	may require compensating controls.
	to verify that	containing both numeric and alphabetic characters.	
	password parameters are set to require	Verizon Business observed system-generated configuration output for the following system	For routers, switches, firewalls, you
	passwords to contain both numeric and	components:	will need
	alphabetic characters.	Cisco ASA 5500 Series-data center	manual reviews to
		Cisco ASA 5585	accomplish,
		Cisco ASA 5540	or use an
		Cisco ASA 5500 Series-store	external AAA
		Cisco ASA 5510	service such
		Cisco Virtual Service Gateway	as TACACS or RADIUS
		Cisco Firewall Services Module	which can
		Cisco routers-store	perform this
		Cisco 891W Cisco 1941W	function for
		Cisco 2921	user
		Cisco 2951	accounts.
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
		Cisco Physical Access Control	

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.	N/A – For the purpose of this assessment, Cisco is not a service provider.		
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------	--	--

8.5.12 Do not allow an	8.5.12.a For a	Verizon Business reviewed	UCS-SRE
individual to submit a new	sample of system	Verizon Business reviewed configuration settings for	may require
password that is the	components, obtain	authentication methods to verify that all PCI Reference	compensating
same as any of the last four	and inspect system	Architecture for Retail Solutions	controls.
passwords	configuration settings	are configured to not allow an individual to submit a new	For routers,
he or she has used.	to verify that	password that is the same as	switches,
he of she has used.	password parameters	any of the last four passwords he or she has used.	firewalls, you
	are set to require that new passwords cannot	Verizon Business observed	will need
	be the same as the	system-generated configuration	manual
	four previously used	output for the following system components:	reviews to accomplish,
	passwords.	Cisco ASA 5500 Series-data	or use an
		center	external AAA
		Cisco ASA 5585	service such
		Cisco ASA 5540 Cisco ASA 5500 Series-store	as TACACS or
		Cisco ASA 5500 Series store	RADIUS
		Cisco Virtual Service Gateway	which can perform this
		Cisco Firewall Services Module	function for
		Cisco routers-store	user
		Cisco 891W	accounts.
		Cisco 1941W	
		Cisco 2921 Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage SwitcheCisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E EMC Ionix Network Configuration	
		Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

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.	N/A – For the purpose of this assessment, Cisco is not a service provider.		
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------	--	--

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.	N/A – For the purpose of this assessment, Cisco is not a service provider.		
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------	--	--

 8.5.15 If a session has been if system or pointers, obtain and inspect system of system components, obtain and inspect system is session. 8.5.15 For a sample of system components, obtain and inspect system is session. 8.5.15 If a session hild the terminal or session. 8.5.15 For a sample of function is uch a way are configured in such as way are configured in such a way are configured in such as way are configured in the such as way are c
Cisco Video Surveillance

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	8.5.16.a Review database and application configuration settings and verify that all users are authenticated prior to access.	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.	
	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).	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.	
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.	
	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).	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.	

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
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	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider. Verizon Business observed		
	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 "locked" to prevent unauthorized use.	verizon Business observed system-generated configuration output for the following system components: Cisco Video Surveillance Cisco Physical Access Control		

9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review	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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.		Verizon Business observed system-generated configuration output for the following system components:	
		Video Surveillance	
Note: "Sensitive areas"		Physical Access Control Manager	
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	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
only point-of-sale terminals are present, such as the cashier areas in a retail store.	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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	least three months. 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.	N/A - Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Identity Services Engine Cisco Identity Services Engine Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960PD Cisco Catalyst 2960PD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560X Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Unified Communications Manager and IP Phones	
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communication s 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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------	
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: requirements, and Revoking terminated onsite personnel and expired visitor badges	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
	9.2.b Verify that access to the badge system is limited to authorized personnel.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
	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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	

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.	token (for example, athe facility to verify the use of visitor ID badges, and thatIbadge or access device)visitor ID badges, and thatSthat expires and thatvisitors are easilydistinguishable from onsite		
	9.3.2.b Verify that visitor badges expire.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
	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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	

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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
	9.5.b Verify that the storage location security is reviewed at least annually.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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).	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	

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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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:	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
	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.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	
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).	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.	

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

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

	PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
--	----------------------	--------------------	----------	--------------	----------

10.1 Establish a	10.1 Verify through	Verizon Business interviewed personnel,	
process for linking all	observation and	reviewed log configuration settings and audit trails of the PCI Reference	
access to system	interviewing the system	Architecture for Retail Solutions to verify	
components	administrator, that audit	that audit trails are enabled and active on	
(especially access	trails are enabled and	all PCI Reference Architecture for Retail Solutions.	
done with	active for system	Verizon Business observed	
administrative	components.	system-generated configuration output for	
privileges such as		the following system components:	
root) to each		Cisco ASA 5500 Series-data center	
individual user.		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 0509 Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager HyTrust Appliance	
		,	
		Cisco Unified Wireless	
		AIR-CT5508 MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready	
		Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	
L		,	

10.2 Implement automated audit trails for all system components to reconstruct the	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the		
following events:	following:		

			1	
10.2.1 All individual	10.2.1 Verify all	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that all individual access to cardholder data		
accesses to	individual access to	audit trails of the PCI Reference		
cardholder data	cardholder data is	Architecture for Retail Solutions to verify		
	logged.	is logged.		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		, 3		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

				-
10.2.2 All actions	10.2.2 Verify actions	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference		
taken by any	taken by any individual	audit trails of the PCI Reference		
individual with root or	with root or	Architecture for Retail Solutions to verify		
administrative	administrative privileges	that actions taken by any individual with root or administrative privileges are logged.		
privileges	are logged.			
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
L		,		

1000			,	
10.2.3 Access to all audit trails	10.2.3 Verify access to	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that access to all audit trails is logged.		
	all audit trails is logged.	audit trails of the PCI Reference		
		Architecture for Retail Solutions to verify that access to all audit trails is longed		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5505		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5500 Series store		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

10.2.4 Invalid logical	10.2.4 Verify invalid	Verizon Business interviewed personnel,	
access attempts	logical access attempts	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify	
	are logged.	Architecture for Retail Solutions to verify	
		that invalid logical access attempts are	
		logged.	
		Verizon Business observed system-generated configuration output for	
		system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager	
		HyTrust Appliance	
		Cisco Unified Wireless AIR-CT5508	
		MSE3550	
		Cisco WCS Manager AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502F	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

			1	
10.2 5 Use of	10.2.5 Verify use of	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify		
identification and	identification and	audit trails of the PCI Reference		
authentication	authentication	Architecture for Retail Solutions to verify		
mechanisms	mechanisms is logged.	that use of identification and authentication mechanisms is logged.		
		55		
		Verizon Business observed system-generated configuration output for		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		, ,		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
L			L L	

10.2.6 Initialization	10 2 6 Vorify	Varizon Rucinoss interviewed personnel		
of the audit logs	10.2.6 Verify initialization of audit logs	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that initialization of audit logs is logged.		
of the addit logs	is logged.	audit trails of the PCI Reference		
	is logged.	Architecture for Retail Solutions to verify that initialization of audit logs is logged		
		Verizon Business observed		
		Verizon Business observed system-generated configuration output for the following system components:		
		the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready		
		Engine		
		Cisco Unified Communications Manager and		
		IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
	I	1	1	1

			1	
10.2.7 Creation and	10.2.7 Verify creation	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that creation and deletion of system level		
deletion of system-level objects	and deletion of system level objects are logged.	audit trails of the PCI Reference		
system-level objects	level objects are logged.	Architecture for Retail Solutions to verify		
		objects are logged.		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585 Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5500 Series store		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager EMC CLARiiON CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		, ,		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

10.3 Record at least	10.3 Through interviews		
the following audit	and observation, for		
trail entries for all	each auditable event		
system components	(from 10.2), perform the		
for each event:	following:		

10.3.1 User	10.3.1 Verify user	Vorizon Business interviewed personnel		
identification	identification is included	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify		
lacitation	in log entries.	audit trails of the PCI Reference		
		that user identification is included in log		
		entries.		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002 Cisco 7206		
		Cisco MDS Storage Switches Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		AIR-LAP1262N		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

			1
10.3.2 Type of event	10.3.2 Verify type of	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify	
	event is included in log	audit trails of the PCI Reference	
	entries.	Architecture for Retail Solutions to verify	
		that type of event is included in log entries.	
		Verizon Business observed system-generated configuration output for	
		the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		, .	
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

			,	
10.3.3 Date and	10.3.3 Verify date and	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify		
time	time stamp is included in	audit trails of the PCI Reference		
	log entries.	Architecture for Retail Solutions to verify		
		that date and time stamp is included in log		
		entries.		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center		
		Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5500 Series-store		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		
	1	,		

10.2.4.0.			1	
10.3.4 Success or	10.3.4 Verify success or	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify		
failure indication	failure indication is included in log entries.	audit trails of the PCI Reference		
	included in log entries.	Architecture for Retail Solutions to verify that success or failure indication is included		
		in log entries.		
		Verizon Business observed		
		system-generated configuration output for the following system components:		
		Cisco ASA 5500 Series-data center Cisco ASA 5585		
		Cisco ASA 5585 Cisco ASA 5540		
		Cisco ASA 5540 Cisco ASA 5500 Series-store		
		Cisco ASA 5500 Series-store		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

10.3.5 Origination of	10.3.5 Verify origination of event is included in	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify	
event	log entries.	audit trails of the PCI Reference	
	log entries.	that origination of event is included in log	
		entries.	
		Verizon Business observed	
		system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5505	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager EMC CLARiiON CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		, 5	
		Cisco Catalyst 6500 Series Intrusion Detection Services Module2	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

			· · · · · · · · · · · · · · · · · · ·
10.3.6 Identity or	10.3.6 Verify identity or	Verizon Business interviewed personnel,	
name of affected	name of affected data,		
data, system	system component, or		
component, or	resources is included in		
resource.	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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that NTP is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	
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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on universally accepted time. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center	
		Cisco ASR 1002 Cisco 7206 Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco switches-store	
		Cisco Catalyst 2960	
		Cisco Catalyst 2960G	
		Cisco Catalyst 2960PD	
		Cisco Catalyst 2960CPD	
		Cisco Catalyst 2960S	
		Cisco Catalyst 3560E	
		Cisco Catalyst 3560X	
		Cisco Catalyst 3560CPD	
		Cisco Catalyst 3750X	
		Cisco Catalyst 4507+R	

10.4.1.b Verify that the designated central time	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that the	
servers peer with each other to keep accurate time, and other internal servers receive time only	designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.	
from the central time servers.	Verizon Business observed system-generated configuration output for the following system components:	
	Cisco routers-store	
	Cisco 891W	
	Cisco 1941W	
	Cisco 2921	
	Cisco 2951	
	Cisco 3945	
	Cisco routers-data center	
	Cisco ASR 1002	
	Cisco 7206	
	Cisco ASA 5500 Series-data center	
	Cisco ASA 5585	
	Cisco ASA 5540	
	Cisco ASA 5500 Series-store	
	Cisco ASA 5510	
	Cisco switches-data center	
	Cisco Catalyst 6509	
	Cisco Catalyst 4948	
	Cisco Nexus 7010	
	Cisco Nexus 5020	
	Cisco switches-store	
	Cisco Catalyst 2960	
	Cisco Catalyst 2960G	
	Cisco Catalyst 2960PD	
	Cisco Catalyst 2960CPD	
	Cisco Catalyst 2960S	
	Cisco Catalyst 3560E	
	Cisco Catalyst 3560X	
	Cisco Catalyst 3560CPD	
	Cisco Catalyst 3750X	
	Cisco Catalyst 4507+R	

			1	
10.4.2 Time data is protected.	10.4.2.a Review system configurations and	Verizon Business reviewed configuration settings of PCI Reference Architecture for		
	time-synchronization	Retail Solutions to verify that access to time data is restricted to only personnel with a		
	settings to verify that	business need to access time data		
	access to time data is restricted to only	Verizon Business observed		
	personnel with a	system-generated configuration output for the following system components:		
	business need to access	Cisco ASA 5500 Series-data center		
	time data.	Cisco ASA 5585		
		Cisco ASA 5540		
		Cisco ASA 5500 Series-store		
		Cisco ASA 5510		
		Cisco Virtual Service Gateway		
		Cisco Firewall Services Module		
		Cisco routers-store		
		Cisco 891W		
		Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		MDS		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager (CSM)		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i AIR-CAP3502E		
		EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System (UCS)		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

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.Verizon Business reviewed configuration settings on critical systems are logged, monitored, and reviewed.Cisco ASA 5500 Series-data center Cisco ASA 5540Cisco ASA 5540Cisco ASA 5510Cisco ASA 5510Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco 1941WCisco 2921 Cisco 2921
synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.
to time settings on critical systems are logged, monitored, and reviewed. Verizon Business observed systems are logged, monitored, and reviewed. Cisco ASA 5500 Series-data center Cisco ASA 5540 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
that any changes to time settings on critical systems are logged, monitored, and reviewed.Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Services Gateway Cisco Firewall Services Module Cisco R91W Cisco 1941W Cisco 2921
settings on critical systems are logged, monitored, and reviewed.
monitored, and reviewed.Cisco ASA 5500 Series-data centerCisco ASA 5585Cisco ASA 5540Cisco ASA 5500 Series-storeCisco ASA 5500 Series-storeCisco ASA 5510Cisco Virtual Service GatewayCisco Firewall Services ModuleCisco routers-storeCisco 704ters-storeCisco 891WCisco 1941WCisco 2921
reviewed. Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921
Cisco 891W Cisco 1941W Cisco 2921
Cisco 1941W Cisco 2921
Cisco 2921
Cisco 2951
Cisco 3945
Cisco routers-data center
Cisco ASR 1002
Cisco 7206
Cisco MDS Storage Switches
Cisco switches-data center
Cisco Catalyst 6509
Cisco Catalyst 4948
Cisco Nexus 7010
Cisco Nexus 5020
Cisco Security Manager (CSM)
HyTrust Appliance
Cisco Unified Wireless
AIR-CT5508
MSE3550
Cisco WCS Manager
AIR-CAP1042N
AIR-CAP3502i
AIR-CAP3502E
EMC Ionix Network Configuration Manager
EMC CLARiiON CX-240
RSA Authentication Manager
RSA Data Protection Manager
RSA enVision
SSL VPN
Cisco Identity Services Engine
Cisco Virtual Service Gateway
Cisco UCS Express on Services Ready Engine
Cisco Unified Communications Manager and IP Phones
Cisco Unified Computing System (UCS)
Cisco Secure Access Control Server
Cisco Video Surveillance
Cisco Physical Access Control

10.4.3 Time settings	10.4.3 Verify that the	Verizon Business reviewed configuration		
are received from	time servers accept time	settings of PCI Reference Architecture for Retail Solutions to verify that the time		
industry-accepted time sources.	updates from specific, industry-accepted	servers accept time updates from specific,		
	external sources (to	industry-accepted external sources. Verizon Business observed		
	prevent a malicious	system-generated configuration output for		
	individual from changing	the following system components:		
	the clock). Optionally,	Cisco ASA 5500 Series-data center		
	those updates can be encrypted with a	Cisco ASA 5585		
	symmetric key, and	Cisco ASA 5540		
	access control lists can	Cisco ASA 5500 Series-store		
	be created that specify	Cisco ASA 5510		
	the IP addresses of client	Cisco Virtual Service Gateway		
	machines that will be provided with the time	Cisco Firewall Services Module		
	updates (to prevent	Cisco routers-store		
	unauthorized use of	Cisco 891W		
	internal time servers).	Cisco 1941W		
		Cisco 2921		
		Cisco 2951		
		Cisco 3945		
		Cisco routers-data center		
		Cisco ASR 1002		
		Cisco 7206		
		Cisco MDS Storage Switches		
		Cisco switches-data center		
		Cisco Catalyst 6509		
		Cisco Catalyst 4948		
		Cisco Nexus 7010		
		Cisco Nexus 5020		
		Cisco Security Manager (CSM)		
		HyTrust Appliance		
		Cisco Unified Wireless		
		AIR-CT5508		
		MSE3550		
		Cisco WCS Manager		
		AIR-CAP1042N		
		AIR-CAP3502i		
		AIR-CAP3502E EMC Ionix Network Configuration Manager		
		EMC CLARIION CX-240		
		RSA Authentication Manager		
		RSA Data Protection Manager		
		RSA enVision		
		Cisco Identity Services Engine		
		Cisco Virtual Service Gateway		
		Cisco UCS Express on Services Ready		
		Engine		
		Cisco Unified Communications Manager and IP Phones		
		Cisco Unified Computing System (UCS)		
		Cisco Secure Access Control Server		
		Cisco Video Surveillance		
		Cisco Physical Access Control		

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:	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions 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	10.5.1 Verify that only individuals who have a	Verizon Business reviewed configuration settings of PCI Reference Architecture for	
with a job-related	job-related need can	Retail Solutions to verify that only	
need.	view audit trail files.	individuals who have a job-related need can view audit trail files.	
		Verizon Business observed	
		system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager EMC CLARiiON CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready	
		Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

	10.5.2 Verify that	Verizon Business reviewed configuration settings of PCI Reference Architecture for	
	current audit trail files are protected from	Retail Solutions to verify that current audit	
	unauthorized	trail files are protected from unauthorized modifications via access control	
	modifications via access	mechanisms, physical segregation, and/or	
	control mechanisms,	network segregation.	
	physical segregation, and/or network	Verizon Business observed system-generated configuration output for the following system components:	
	segregation.	Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Video Surveillance	
1 1		Cisco Physical Access Control	

10.5.3 Promptly back	10.5.3 Verify that	Verizon Business reviewed configuration settings of PCI Reference Architecture for	
up audit trail files to a	current audit trail files	Retail Solutions to verify that current audit	
centralized log server or media	are promptly backed up to a centralized log	trail files are promptly backed up to a	
	server or media that is	centralized log server that is difficult to alter.	
that is difficult to	difficult to alter.	Verizon Business observed	
alter.		system-generated configuration output for the following system components:	
		Cisco ASA 5500 Series-data center	
		Cisco ASA 5585	
		Cisco ASA 5540	
		Cisco ASA 5500 Series-store	
		Cisco ASA 5510	
		Cisco Virtual Service Gateway	
		Cisco Firewall Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
		Cisco routers-data center	
		Cisco ASR 1002	
		Cisco 7206	
		Cisco MDS Storage Switches	
		Cisco switches-data center	
		Cisco Catalyst 6509	
		Cisco Catalyst 4948	
		Cisco Nexus 7010	
		Cisco Nexus 5020	
		Cisco Security Manager (CSM)	
		HyTrust Appliance	
		Cisco Unified Wireless	
		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager	
		AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		EMC Ionix Network Configuration Manager	
		EMC CLARIION CX-240	
		RSA Authentication Manager	
		RSA Data Protection Manager	
		RSA enVision	
		Cisco Identity Services Engine	
		Cisco Virtual Service Gateway	
		Cisco UCS Express on Services Ready Engine	
		Cisco Unified Communications Manager and IP Phones	
		Cisco Unified Computing System (UCS)	
		Cisco Secure Access Control Server	
		Cisco Video Surveillance	
		Cisco Physical Access Control	

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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that logs for external-facing technologies are sent to a secure centralized internal log server.		
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.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that use of file-integrity monitoring software for logs by examining system settings and monitored files and results from monitoring activities. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Communications Manager and IP Phones Cisco Video Surveillance Cisco Physical Access Control Cisco Unified Computing System (UCS) RSA Authentication Manager Cisco Security Manager EMC Ionix Network Configuration Manager RSA Data Protection Manager Cisco MDS Storage Switches EMC CLARiiON CX-240 Cisco Secure Access Control Server	This requirement is met by the use of the RSA enVision server aggregating each of the device logs and file integrity monitoring being provided by the RSA enVision software.	
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,	 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 	N/A – Policies and Procedures is the responsibility of the merchant / service provider. Verizon Business reviewed configuration		
authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to	observation and interviews, verify that regular log reviews are performed for all system components.	settings of PCI Reference Architecture for Retail Solutions to verify that log aggregation solutions generate events and alerts which are reviewed daily.		
meet compliance with Requirement 10.6.				

OL-13453-01

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	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.	N/A – Security Policy (Data Retention) is the responsibility of the merchant / service provider.	
restorable from back-up).	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.	Verizon Business reviewed online logs and audit trail archive methods within the PCI Reference Architecture for Retail Solutions environment to confirm that audit trails can be retained for at least one year, with at least three months available online.	

Requirement 11: Regularly test security systems and processes.

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	11.1.a Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.	Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.		
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/.				
Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.				

11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable wireless devices connected to system components (for example, by USB, etc.) Wireless devices attached to a network port or network device	Verizon Business verified 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 Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E Cisco Identity Services Engine Cisco switches-store Cisco Catalyst 2960	
	Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R	
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.	N/A – Policy and procedures is the responsibility of the merchant / service provider.	

	1.1.d If automated nonitoring is utilized	Verizon Business verified If automated monitoring is utilized, the configuration	
(fe	or example,	will generate alerts to personnel.	
	wireless IDS/, NAC, etc.), verify the configuration will generate alerts to personnel.	Verizon Business observed	
cc		system-generated configuration output for the following system components:	
<u> </u>		Cisco Unified Wireless	
p		AIR-CT5508	
		MSE3550	
		Cisco WCS Manager AIR-CAP1042N	
		AIR-CAP3502i	
		AIR-CAP3502E	
		AIR-LAP1262N	
		Cisco Identity Services Engine	
		Cisco switches-store	
		Cisco Catalyst 2960	
		Cisco Catalyst 2960G	
		Cisco Catalyst 2960PD	
		Cisco Catalyst 2960CPD	
		Cisco Catalyst 2960S	
		Cisco Catalyst 3560E	
		Cisco Catalyst 3560X	
		Cisco Catalyst 3560CPD	
		Cisco Catalyst 3750X	
		Cisco Catalyst 4507+R N/A – Incident Response policy and	
4.	1 1 a Varify the	procedures is the response policy and	
	1.1.e Verify the rganization's	merchant / service provider.	
in	ncident response		
	lan (Requirement 2.9) includes a		
re	esponse in the event		
-	nauthorized wireless evices are detected.		
ŭ			

11.2 Kun internal and 11.2 Verify that internal and external vulnerability scans after any significant change in the restorek (such as new system component Installations, changes in network (such as new system component Installations, changes in network (such as new system component Installations, changes in network (such as new required that four passing quarterly scans must be completed for initial PCI DSS complane if the assessor verifies scan result was a passing scan, j) the entity 11.2.1.a Review the scan reports and verify that four quarterly internal scans reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.3 Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.5 Review the scan reports and verify that the scan process includes rescuts are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.6 Review the scan reports and verify that the scan process includes resource(s) or qualified internal independence of the tester exists (not required to be a QSA N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.				1	
vulnerability scans at after any significant change in the metwork (such as new system component Installations, changes in network topology, frewall rule ungrades). vulnerability scans follows: Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies scan result was a passing scan, 2) the entity N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Ferform quarterly internal scan reports and verify that four quarterly internal scan reports and verify that four quarterly that four quarterly internal scan reports and verify that the scan process includes rescans until passing rescue is a contral in the provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
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 11.2.1.8 Review the scan reports and verify that four guarterly internal scans occurred in the most recent 12-month period. 11.2.1.9 Review the scan reports and verify that the scan process includes recaus us and basing recaus a ubt passing recaus number obtained, or all "High" underballities as defined in PCI DSS Requirement 6.2 are resolved. NA - Internal quarterly scanning is the responsibility of the merchant / service provider. NA - Internal quarterly scanning is the responsibility of the merchant / service provider. NA - Internal quarterly scanning is the responsibility of the merchant / service provider. NA - Internal quarterly scanning is the responsibility of the merchant / service provider.					
after any significant change in the system component system component in network (such as new system component installations, changes in network topology, frewall rule modifications, product upgrades). follows: Note: It is not required that four passing quartery scans must be completed for initial PCI DSS compliance if the assessor verifies scan reports and vulnerability scans. 11.2.1.a Review the scan reports and vulnerability scans. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Perform quarterly internal scan soccurred in the most recent 12.2.1 perform quarterly internal scan soccurred in the most recent 12.1.1 perform quarterly that four quarterly that four quarterly that four quarterly internal scan soccurred in the most recent 12.1.1 perform vulnerability scans. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.1 Call Call date that the scan verify or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.	,				
change in the network (such as new system component Installations, changes in network topology, frewall rule modifications, product upgrades). Note: It is not required that four passing quartery scans must breach PCI DSS complance if the assessor verifies J1 the most recent scan reputs and vulnerability scans. 11.2.1.8 Review the scan reputs and vulnerability scans. 11.2.1.8 Review the scan reports and verify that four quartery internal scans occurred in the most recent 12-month period. 11.2.1.1 Review the scan reports and verify that the scan process includes resons until passing resolved. 11.2.1.2.1.4 Review the scan reports and verify that the scan process includes resons until passing resolved. 11.2.1.2.1.4 Review the scan reports and verify that the scan process includes resolved. 11.2.1.2.1.6 Review the scan reports and verify that the scan process includes resolved. 11.2.1.1.3.1.C Validate that the scan was performed by a qualified internal resolved. 11.2.1.4 Review the scan reports and verify that the scan process includes resolved. 11.2.1.6 Review the scan reports and verify that the scan process includes resolved. 11.2.1.6 Review the scan reports and verify that the scan was performed by a qualified internal resolved. 11.2.1.6 Review the scan reports and verify that the scan was performed by a qualified internal resolved. 11.2.1.6 Review the scan reports and verify that the scan was performed by a qualified internal resolved. 11.2.1.6 Review the that the scan was performed by a qualified internal resolved. 11.2.1.6 Review the that the scan was performed by a qualified internal resolved. 11.2.1.6 Review the scan reports of the the ster exist (not					
network (such as new system component Installations, changes in network topology, frewall 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 11.2.1 Perform quarterly internal vulnerability scans. 11.2.1.5. Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. 11.2.1.5. Review the scan reports and verify that the scan process includes results are obtained, or all "High" vulnerability is cans. 11.2.1.C.V Review the scan reports and verify that the scan process includes results are obtained, or all "High" vulnerability of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.		follows:			
system component Installations, changes in network topology, frewail 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 11.2.1 Perform quarterly internal scans reports and verify that the scan process includes responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.	change in the				
system component Installations, changes in network topology, frewail rule modifications, product uggrades). 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 11.2.1 Perform quarterly internal scans cocurred in the most recent I2-month period. 12.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	network (such as new				
Installations, changes in network topology, frewall rule modifications, product upgrades). Note: It is not required that four passing quarterly cans 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 11.2.1 Perform vulnerability scans. I 1.2.1 Perform vulnerability scans. I 1.2.1 Perform vulnerability scans. I 1.2.1 Perform vulnerability scans. NA - Internal quarterly scanning is the responsibility of the merchant / service provider. NA - Internal quarterly scanning is the responsibility of the merchant / service provider.					
in network topology, frewall 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 11.2.1 Perform quarterly internal vulnerability scans. I 1.2.1.8 Review the scan reports and verify that four quarterly internal scan soccurred in the most recent 12-month period. I 1.2.1.8 Review the scan reports and verify that four quarterly internal vulnerability scans. I 1.2.1.8 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. I 1.2.1.6 Validate that the scan was performed by a qualified internal resource(s) or qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the test exists (not	, ,				
frewall 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 11.2.1 Perform quarterly internal vulnerability scans. I 12.2.1 Perform quarterly internal scans occurred in the most recent 12-month period. I 12.1.16 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. I 12.1.12 Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the test exkiss (not					
modifications, product upgrades). N/A = Internal quarterly scanning is the 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 11.2.1.a Review the lass documented N/A = Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.B Review the quarterly internal scan reports and verify that four quarterly internal scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" N/A = Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.D Review the defined in PCI DSS Requirement 6.2 are resoluted. N/A = Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.C Validate that the scan was performed by a qualified internal resource(s) or qualified internal resource(s) or qualified internal resource(s) or qualified internal resource(s) or qualified internal independence of the tester exists (not N/A = Internal quarterly scanning is the resonsibility of the merchant / service					
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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 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 scan reports and verify that four quarterly internal scans occurred in the scan reports and verify that the scan verify that the scan reports and verify that the scan verify that the scan verify tha					
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 III.2.1.8 Review the scan reports and vulnerability scans. III.2.1.8 Review the scan reports and vulnerability scans. III.2.1.8 Review the scan reports and vulnerability scans. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. III.2.1.9 Review the scan reports and vulnerability scans. III.2.1.8 Review the scan reports and verify that four quarterly internal scan reports and vulnerability active the scan reports and vulnerability are obtained, or all "tight" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. III.2.1.5 Review the scan reports and vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. III.2.1.5 Review the scan reports and verify that the scan process includes rescan und passing results are obtained, or all "tight" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. III.2.1.C validate that the scan was performed by a qualified external third party, and if applicable, organizational independence of the tester exists (not					
required that four passing quaterly 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 11.2.1 Perform quarterly internal scans occurred in the most recent 12-month period. 11.2.1 keview the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. 11.2.1 keview the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" ulmerabilities 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 internal resource(s) or qualified chernal third party, and if applicable, organizational independence of the tester exists (not	upgrades).				
required that four passing quaterly 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 11.2.1 Perform quarterly internal scans occurred in the most recent 12-month period. 11.2.1 keview the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. 11.2.1 keview the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" ulmerabilities 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 internal resource(s) or qualified chernal third party, and if applicable, organizational independence of the tester exists (not	Note: It is not				
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 Nas documented 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 to scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS defined in PCI DSS Requirement 6.2 are resolved. 11.2.1.c Validate that the scan was performed by a qualified internal rescurse(s) or qualified internal resource(s) or qualified inte					
scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan reports and verify that four unierability scans.	-				
completed for initial PCI DSS compliance if the assessor verifies and the most recent 1) the most recent scan result was a passing scan, 2) the ntable 11.2.1 Perform 11.2.1.a Review the vulnerability scans. 11.2.1.a Review the vulnerability scans. 11.2.1.b Review the vulnerability scans. 11.2.1.b Review the scan result were responsibility of the merchant / service provider. provider. 11.2.1.b Review the scan reports and verify that four provider. 11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing responsibility of the merchant / service provider. provider. vulnerabilities as defined in PCI DSS Requirement 6.2 are responsibility of the merchant / service performed by a qualified aternal that the scan was performed by a qualified internal responsibility of the merchant / service provider. provider. qualified external thind party, and if					
PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented 11.2.1 Perform quarterly internal scans occurred in the most recent 12-month period. 11.2.1.b 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					
the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented 11.2.1 Perform quarterly internal vulnerability scans.					
1) the most recent scan result was a passing scan, 2) the entity II.2.1 a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Perior N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Perior N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Perior N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Perior N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 Collidate that the scan process includes resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1 collidate 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service					
scan result was a passing scan, 2) the entity II.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. II.2.1.b Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. II.2.1.b Review the scan reports and verify that bescan reports and verify that the scan reports and verify that the scan reports and verify that can process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. II.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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
passing scan, 2) the entity Image: scan regords and verify that the scan reports and verify 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service					
entity has documented 11.2.1 Perform quarterly internal vulnerability scans. 11.2.1. 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 external third party, and if applicable, organizational independence of the tester exists (not					
has documented II.2.1 Perform II.2.1 a Review the N/A - Internal quarterly scanning is the quarterly internal verify that four quarterly internal responsibility of the merchant / service vulnerability scans. II.2.1.a Review the N/A - Internal quarterly scanning is the responsibility of the merchant / service 12-month period. II.2.1.b Review the N/A - Internal quarterly scanning is the responsibility of the merchant / service verify that the scan process includes N/A - Internal quarterly scanning is the responsibility of the merchant / service vulnerabilities as defined in PCI DSS Requirement 6.2 are responsibility of the merchant / service II.2.1.C Validate N/A - Internal quarterly scanning is the responsibility of the merchant / service responsibility of the merchant / service qualified internal responsibility of the merchant / service responsibility of the merchant / service responsibility of the merchant / service qualified internal responsibility of the merchant / service qualified internal responsibility of the merchant / service responsibility of the merchant / service responsibility of the merchan					
11.2.1 Perform 11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.b Review the scan reports and verify that the scan reports and verify that 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. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.C Validate that the scan pprocess includes resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.C Validate that the scan performed by a qualified internal resource(s) or qualified internal resource(s) or qualified internal resource(s) or qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
quarterly internal vulnerability scans. scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. responsibility of the merchant / service provider. 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. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
vulnerability scans. verify that four quarterly internal scans occurred in the most recent 12-month period. provider. 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. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
quarterly internal scans occurred in the most recent 12-month period.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.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.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.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 (notN/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
scans occurred in the most recent 12-month period.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.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.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.11.2.1.c Validate that the scan was performed by a qualified internal responsibility of the merchant / service provider.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.11.2.1.c Validate that the scan was performed by a qualified internal responsibility of the merchant / service provider.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.11.2.1.c validate that the scan was performed by a qualified internal responsibility of the merchant / service provider.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.	vulnerability scans.		provider.		
most recent 12-month period.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.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.N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.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 (notN/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
12-month period. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 11.2.1.b Review the scan percess includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the responsibility of the merchant / service provider. 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
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. N/A - Internal quarterly scanning is the responsibility of the merchant / service 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service					
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.responsibility of the merchant / service provider.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 (notN/A - Internal quarterly scanning is the responsibility of the merchant / service		12-month period.			
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.provider. 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 (notN/A - Internal quarterly scanning is the resons the merchant / service provider.		11.2.1.b Review the			
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		scan reports and	responsibility of the merchant / service		
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		verify that the scan	provider.		
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		process includes			
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					
vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.					
defined in PCI DSS Requirement 6.2 are Requirement 6.2 are resolved. 11.2.1.c Validate N/A - Internal quarterly scanning is the that the scan was responsibility of the merchant / service performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not resists (not					
Requirement 6.2 are resolved. N/A - Internal quarterly scanning is the 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 N/A - Internal quarterly scanning is the responsibility of the merchant / service provider.		vulnerabilities as			
resolved. I1.2.1.c Validate N/A - Internal quarterly scanning is the that the scan was responsibility of the merchant / service performed by a provider. qualified internal provider. resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not resolved.					
11.2.1.c Validate N/A - Internal quarterly scanning is the that the scan was responsibility of the merchant / service performed by a provider. qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not		Requirement 6.2 are			
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		resolved.			
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		11.2.1.c Validate	N/A – Internal guarterly scanning is the		
performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not					
qualified internalresource(s) orqualified externalthird party, and ifapplicable,organizationalindependence of thetester exists (not					
resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not					
qualified external third party, and if applicable, organizational independence of the tester exists (not					
third party, and if applicable, organizational independence of the tester exists (not					
applicable, organizational independence of the tester exists (not					
organizational independence of the tester exists (not					
independence of the tester exists (not					
tester exists (not					
11.2.2 Perform	11.2.2.a Review	N/A – Third party external, quarterly			
-------------------------	----------------------------	---------------------------------------	--		
quarterly external	output from the four	scanning is the responsibility of the			
vulnerability scans via	most recent guarters	merchant / service provider.			
an Approved Scanning	of external	merchant / service provider.			
Vendor (ASV),	vulnerability scans				
approved by the	and verify that four				
Payment Card	guarterly scans				
Industry Security	occurred in the most				
Standards Council	recent 12-month				
(PCI SSC).					
(PCI 55C).	period.				
	11.2.2.b Review the	N/A – Third party external, quarterly			
Note: Quarterly	results of each	scanning is the responsibility of the			
external vulnerability	quarterly scan to	merchant / service provider.			
scans must be	ensure that they				
performed by an	satisfy the ASV				
Approved Scanning	Program Guide				
Vendor (ASV),	requirements (for				
approved by the	example, no				
Payment Card	vulnerabilities rated				
Industry Security	higher than a 4.0 by				
Standards Council	the CVSS and no				
(PCI SSC). Scans					
conducted after	11.2.2.c Review the	N/A – Third party external, quarterly			
	scan reports to verify	scanning is the responsibility of the			
network changes may	that the scans were	merchant / service provider.			
be performed by	completed by an				
internal staff.	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.	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.	
	11.2.3.b Review scan reports and verify that the scan process includes rescans until:	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.	
	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).	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.	

11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub- network added to the environment, or a web server added to the environment). These penetration tests must include the following:	 11.3.a Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. 11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated. 	N/A – Penetration Testing is the responsibility of the merchant / service provider. N/A – Penetration Testing is the responsibility of the merchant / service provider.	
	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	N/A – Penetration Testing is the responsibility of the merchant / service provider.	
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.	N/A – Penetration Testing is the responsibility of the merchant / service provider.	
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.	N/A – Penetration Testing is the responsibility of the merchant / service provider.	

11.4 Use	11.4.a Verify the use	Verizon Business reviewed all IDS/ within	
intrusion-detection systems, and/or	of intrusion-detection systems and/or	the PCI Reference Architecture for Retail Solutions environment and confirmed	
intrusion-prevention	intrusion-prevention	that all traffic at the perimeter of the	
systems to monitor all	systems and that all	cardholder data environment as well as at	
traffic at the perimeter	traffic at the	critical points in the cardholder data	
of the cardholder data	perimeter of the	environment is monitored.	
environment as well	cardholder data		
as at critical points inside of the	environment as well as at critical points in	Verizon Business observed	
cardholder data	the cardholder data	system-generated configuration output	
environment, and	environment is	for the following system components:	
alert personnel to	monitored.		
suspected		Cisco ASA 5500 Series-data center	
compromises. Keep all		Cisco ASA 5585	
intrusion-detection		Cisco ASA 5540	
and prevention engines, baselines,		Cisco ASA 5500 Series-store	
and signatures		Cisco ASA 5510	
up-to-date.		Cisco Intrusion Detection Services Module	
		Cisco routers-store	
		Cisco 891W	
		Cisco 1941W	
		Cisco 2921	
		Cisco 2951	
		Cisco 3945	
	11.4.b Confirm IDS	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail	
	and/or are configured to alert	Solutions environment and confirmed	
	personnel of	that they are configured to alert	
	suspected	personnel of suspected compromises.	
	compromises.		
	11.4.c Examine IDS/	Verizon Business reviewed all IDS/ within	
	configurations and	the PCI Reference Architecture for Retail	
	confirm IDS/ devices	Solutions environment and confirmed	
	are configured,	that they are configured, maintained, and	
	maintained, and	updated per vendor instructions to ensure	
	updated per vendor instructions to ensure	optimal protection.	
	optimal protection.		
	1		

			1
11.5 Deploy	11.5.a Verify the use	Verizon Business reviewed FIM settings,	
file-integrity	of file-integrity	monitored files, and results from	
monitoring tools to	monitoring tools within the cardholder	monitoring activities within the PCI Reference Architecture for Retail	
alert personnel to unauthorized	data environment by	Solutions environment and verified that	
modification of critical	observing system	file-integrity monitoring tools are used.	
system files,	settings and	me-integrity monitoring tools are used.	
configuration files, or	monitored files, as		
content files; and	well as reviewing		
configure the software	results from		
to perform critical file	monitoring activities.		
comparisons at least	Examples of files that		
weekly.	should be monitored:		
Notos Forfilo integrity	System		
Note: For file-integrity monitoring purposes,	executables		
critical files are usually	Application		
those that do not	executables		
regularly change, but	Configuration and		
the modification of	parameter files		
which could indicate a	Centrally stored,		
system compromise or	historical or archived,		
risk of compromise.	log and audit files		
File-integrity	11.5.b Verify the	Verizon Business reviewed FIM settings,	
monitoring products usually come	tools are configured	monitored files, and results from	
pre-configured with	to alert personnel to	monitoring activities within the PCI	
critical files for the	unauthorized	Reference Architecture for Retail	
related operating	modification of critical	Solutions environment and verified that	
system. Other critical	files, and to perform	FIM is to be configured to alert personnel	
files, such as those for	critical file comparisons at least	to unauthorized modification of critical files, and to perform critical file	
custom applications,	weekly.	comparisons at least weekly by the	
must be evaluated and	weekiy.	merchant or service provider.	
defined by the entity			
(that is, the merchant			
or service provider).			

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
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).	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.	N/A – Security Policy is the responsibility of the merchant / service provider.		
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.	N/A – Security Policy is the responsibility of the merchant / service provider.		
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.	N/A – Security Policy is the responsibility of the merchant / service provider.		
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.	N/A – Security Policy is the responsibility of the merchant / service provider.		

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.	N/A – Security Policy and Procedures is the responsibility of the merchant / service provider.	
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.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.	
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).	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.	
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.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.	
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.	N/A – Acceptable Use Policy / Asset List is the responsibility of the merchant / service provider.	
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies require acceptable uses for the technology.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.	
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies require acceptable network locations for the technology.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.	

12.3.7 Verify that the usage	N/A – Acceptable Use Policy		
policies require a list of company- approved products.	is the responsibility of the merchant / service provider.		
12.3.8 Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
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.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
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.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
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.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.4 Verify that information security policies clearly define information security responsibilities for all personnel.	N/A – Security Policy is the responsibility of the merchant / service provider.		
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:	N/A – Security Policy is the responsibility of the merchant / service provider.		
	 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 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.a Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. 12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. 12.4 Verify that information security policies clearly define information security responsibilities for all personnel. 12.5 Verify the formal assignment of information 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 	12.3.8 Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.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.N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.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.N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.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.N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.12.4 Verify that information 	12.3.8 Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider. 12.3.9 Verify that the usage policies require activation of remote- access technologies aget by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider. 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 excessing such data via remote-access technologies. N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider. 12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCL DSS Requirements. N/A - Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider. 12.4 Verify that information security policies clearly define information security responsibilities for all personnel. N/A - Security Policy is the responsibility of the merchant / service provider. 12.5 Verify the formal assignment of information security-knowledgeable member of management. N/A - Security Policy is the responsibility of the merchant / service provider. 0btain and examine information security pofficer or other security responsibilities are specifically and formality N/A - Security Policy is the responsibility of the merchant / service provid

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.	N/A – Security Policy is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy (Risk / Vulnerability management) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy (Risk / Vulnerability management) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy (ID / Account management) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy (Data Control / Monitoring) is the responsibility of the merchant / service provider.	
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.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.	
	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).	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.	

	12.6.1.b Verify that personnel attend awareness training	N/A – Security Policy (Security Awareness) is the	
	attend awareness training upon hire and at least annually.	responsibility of the merchant / service provider.	
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.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.	
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.)	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.	N/A – Security Policy (Background Checks) is the responsibility of the merchant / service provider.	
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.			
12.8 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.	N/A – Connected Entity List (List of Service Providers with whom cardholder data is shared) is the responsibility of the merchant / service provider.	

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.	N/A – Third party contracts is the responsibility of the merchant / service provider.	
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.	N/A – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the merchant / 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.	N/A – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the merchant / service provider.	
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	 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 	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
compromises Coverage and responses of all critical system components Reference or inclusion of incident response procedures from the payment brands	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		

	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.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
12.9.2 Test the plan at least annually.	12.9.2 Verify that the plan is tested at least annually.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
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.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
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 responsibilities for security breach response is periodically trained.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
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.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	
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.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.	