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

Verizon Business **Rob McIndoe** *Sr. Security Consultant* *CISSP, PCI QSA, PA-QSA, CISA, GSEC* robert.mcindoe@verizonbusiness.com	verizonbusiness Security Solutions powered by Cybertrust
Cisco *Customer contact information*	**Customer logo**

1. Executive Summary

Architecture Description

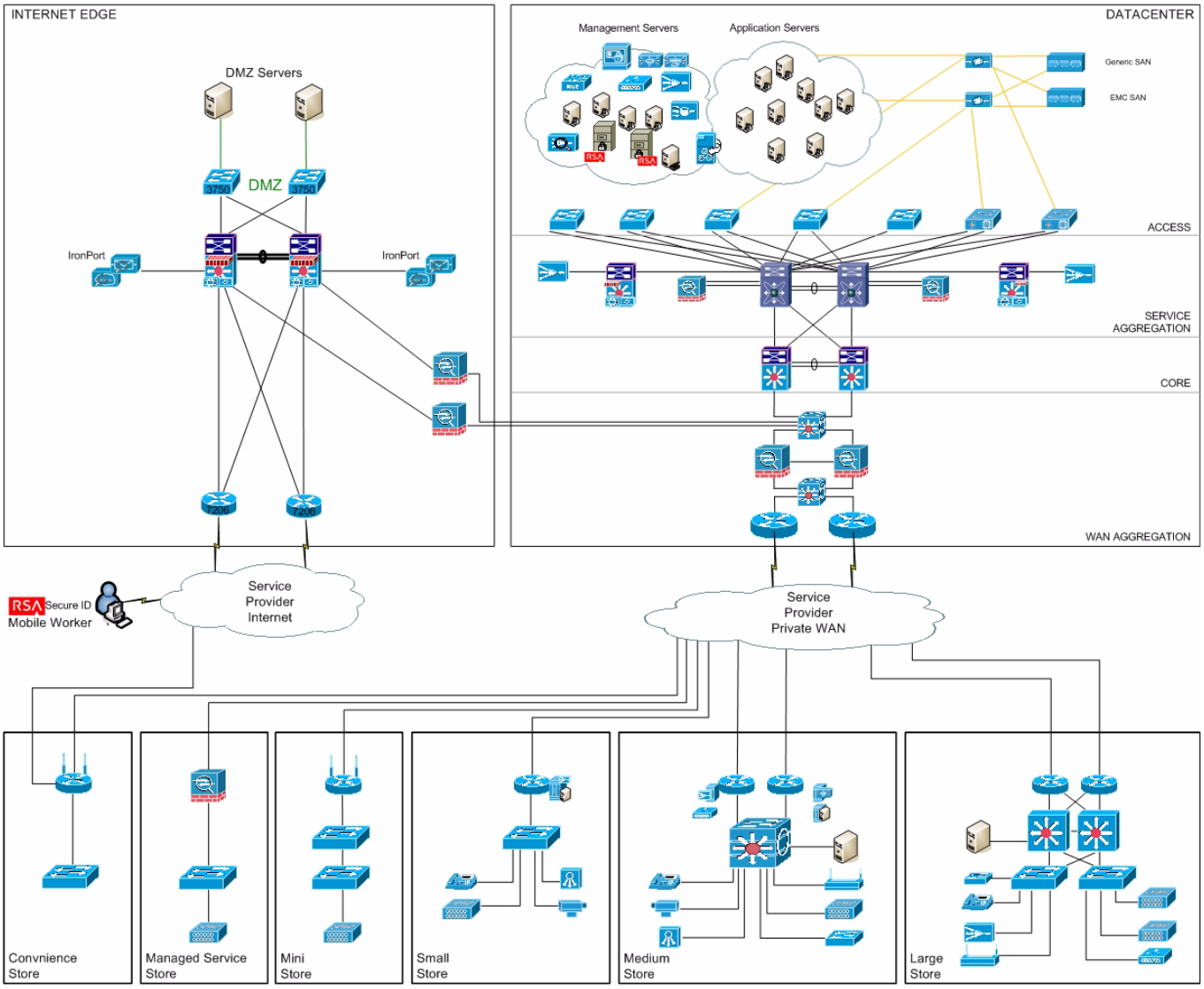
Cisco Systems, Inc engaged Verizon Business to conduct a PCI reference architecture assessment of their "PCI Solution for Retail" designed architecture, based on the PCI DSS v2.0 standard. The architecture assessment against the PCI DSS v2.0 standard included a review of the Cisco PCI Solution for retail 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	CUCM
Mourad Cherfaoui	CUCM

Danny Dhillon	RSA enVision
Danny Dhillon	RSA Authentication Manager
Danny Dhillon	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** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	N/A – Firewall/Router configuration 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.		
	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 router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. **Note:** An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	Verizon Business reviewed access lists across firewalls and routers and verified that inbound and outbound traffic is limited to that which is necessary for a 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 Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		Configurations for perimeter firewalls/routers outside the PCI Solution for Retail environment are the responsibility of merchant / service provider.
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	Verizon Business reviewed access lists across firewalls and routers and verified that all other inbound and outbound traffic is specifically denied. 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		

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		

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Verizon Business reviewed network topologies and access lists across firewalls and routers and verified that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, 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		

1.3.2 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. 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		Perimeter firewall/router configurations and rule sets are the responsibility of the merchant / service provider.

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 unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized	Verizon Business reviewed outbound access-lists from the PCI Reference Architecture for Retail Solutions environment and confirmed that all outbound traffic is destined for "data 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 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		

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)	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. 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 unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* *Network Address Translation (NAT)* *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* *Removal or filtering of route advertisements for private networks that employ registered addressing,* *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Verizon Business reviewed DHCP reservations, static IPs, and access lists across firewalls and routers and confirmed that RFC 1918 addresses were used within the PCI Solution for Retail 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		
	1.3.8.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 employee-owned computers.	**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.		

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 Requirements	Testing Procedures	In Place	Not in Place	Comments
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 default passwords/passphrases on access points were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: 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 firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: WPA technology is enabled (WPA/TKIP w/PEAP authentication).		
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: 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 configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST)	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. 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 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.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. 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 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 configured.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: 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 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.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).			
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		
	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.		

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or ec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.	Verizon Business reviewed configuration settings for PCI Reference Architecture for Retail Solutions and verified that that only necessary services or protocols are enabled. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS 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 Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		.

	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.	Verizon Business reviewed configuration settings for PCI Reference Architecture for Retail Solutions and verified that insecure services and protocols are not used. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS 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		

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 are included in the system configuration standards.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. 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 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		Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.

	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	Verizon Business reviewed configuration settings across all PCI Reference Architecture for Retail Solutions and confirmed they were based on best practice standards, and that common security parameters were set appropriately. Verizon Business also confirmed all management consoles were configured to support secure access (e.g. SSH, https, High-Encryption RDP), and that http, Telnet, and other insecure protocols commonly used for administrative access had been disabled. Additionally, role-based administration was configured for administration of the PCI 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 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 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		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and verified that they were based on best practice standards, and that all unnecessary functionality was disabled. 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 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		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

	2.2.4.b. Verify enabled functions are documented and support secure configuration.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and confirmed that enabled functions are documented and support secure configuration. 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 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		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

	2.2.4.c. Verify that only documented functionality is present on the sampled system components.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and confirmed that only documented functionality is present on the sampled system 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 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		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

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 administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that strong encryption methods are invoked before the administrator's password is requested. 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 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		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.

	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that Telnet and other remote login commands are not available for use internally. 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 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		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.

	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that administrator access to the web-based management interfaces is encrypted with strong cryptography. 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 Video Surveillance		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	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 verify that stored cardholder data does not exceed requirements defined in the data retention policy.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		

	3.1.1.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.	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).		
	3.2.c For each item of sensitive authentication data below, perform the following steps:			

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

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 encryption.		
	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).	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 (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).	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.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 the solution.		
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: **Note:** This requirement also applies to key-encrypting keys used to protect data- encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	N/A – Protection of encryption keys is the 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/decryption purposes. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.	N/A – Protection of encryption keys is the responsibility of the merchant / 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-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.	N/A – Protection of encryption keys is the responsibility of the merchant / service provider. Verizon Business observed system-generated 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: **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data.	N/A – Key Management policy and procedures is the responsibility of the merchant / service provider.		
	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/256-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 distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.	N/A – Key Management 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 time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. 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 (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that destruction of 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, or delete, when necessary.		
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.	N/A – Key Management policies and procedures is the 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 necessary.		

	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.	N/A – Key Management policies and procedures is the responsibility of 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 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		

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). **Note:** Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that split knowledge/dual control 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.		

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 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 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. **Note:** The use of WEP as a security control was prohibited as of 30 June 2010.	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	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. 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		

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:	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.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.	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

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. **Note:** An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.	Verizon Business reviewed configurations for the PCI Reference Architecture for Retail Solution components, including management consoles for components within the PCI Solution for Retail environment and confirmed they are running current software releases and contain current vendor patches as of the time of this assessment. 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		

	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 above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component. The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At	N/A – Patch / Risk management policy and procedures is the responsibility of the merchant / service provider.		
	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	N/A – Software Development was not in scope for this assessment.		
	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.		
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with	N/A – Software Development was not in scope for this assessment.		
	6.3.d From an examination of 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 prior to release to production or customers in order to identify any potential coding vulnerability. **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	**6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). Appropriate corrections are implemented prior to release.	N/A – Software Development was not in scope for this assessment.		
	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	N/A – Software Development was not in scope for this assessment.		

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

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.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.	N/A – Security 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 practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	**6.5.a**Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and	N/A – Software Development is not in scope for assessment.		
	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.		
	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:			

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	N/A – Software Development is not in scope for assessment.		
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)	N/A – Software Development is not in scope for assessment.		
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)	N/A – Software Development is not in scope for assessment.		
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)	N/A – Software Development is not in scope for assessment.		
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)	N/A – Software Development is not in scope for assessment.		
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.	N/A – Software Development is not in scope for assessment.		
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 scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	N/A – Software Development is not in scope for assessment.		

6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object	N/A – Software Development is not in scope for assessment.		
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically	N/A – Software Development is not in scope for assessment.		

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Installing a web-application firewall in front of public-facing web applications	**6.6** For public-facing web applications, ensure that either one of the following methods are in place as follows: Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. **Note:** "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.	N/A – Public-facing web applications are not in scope for assessment.		

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 rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	Verizon Business confirmed privileged user IDs are restricted to the least privileges necessary to perform job functions and 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 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		

7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).	Verizon Business confirmed privileges are assigned to roles that 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 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		

7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.	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		

7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.	Verizon Business confirmed automated access controls 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 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. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			

7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.	Verizon Business reviewed system components and verified that access control 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 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		

7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	Verizon Business reviewed system components and verified that access control systems include role-based privilege assignment for 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 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		

7.2.3 Default "deny-all" setting **Note:** Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.	Verizon Business reviewed system components and verified that access control systems include default "deny-all" settings 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 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 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		

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	Comments

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.	Verizon Business reviewed 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 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		

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 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		

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial- in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) **Note:** Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.	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.

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.	Verizon Business reviewed configuration settings of all PCI Reference Architecture for Retail Solution components and verified that passwords are unreadable during 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		

	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 from the authorization 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/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.	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.		

8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.	N/A – Manual audit procedure or third party ID management tool is the responsibility of the merchant / service provider. 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

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.		

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: Generic user IDs and accounts are disabled or removed Shared user IDs for system administration activities and other critical functions do not exist Shared and generic user IDs are not used to administer any system components	Verizon Business reviewed user 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 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 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		

	8.5.8.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 passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to change user passwords at least every 90 days. 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	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.	N/A – For the purpose of this assessment, Cisco is not a 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 password parameters are set to require passwords to be at least seven characters long.	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. 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		UCS-SRE may require compensating controls

	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 containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to use passwords containing both numeric and alphabetic characters. 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	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 individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. 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 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	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 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to limit repeated access attempts by locking out the user ID after not more than six attempts. 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 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	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.		

8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. 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 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		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured in such a way that If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. 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 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		

8.5.16 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 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.	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 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 collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. **Note:** "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	**9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.	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: Video Surveillance Physical Access Control Manager		
	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.		
	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.	**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 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 Cisco Unified Communications Manager and IP Phones		

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	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.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	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 process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that audit trails are enabled and active on all PCI 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 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		

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

10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	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 is 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		

10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that actions taken by any individual with root or administrative 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		

10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	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. 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		

10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that invalid logical access attempts 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		

10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that use of identification and authentication mechanisms is 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		

10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.	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. 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		

10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	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 objects 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		

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

10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify 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		

10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference 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 time	**10.3.3** Verify date and time stamp is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference 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 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		

10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference 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 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		

10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify 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 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		

10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	Verizon Business interviewed personnel,		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **Note:** One example of time synchronization technology is Network Time Protocol (NTP).	**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.		
	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 servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only 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		

10.4.2 Time data is protected.	**10.4.2.a** Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that access to time data is restricted to only personnel with a business need to access time data 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 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 of PCI Reference Architecture for Retail Solutions to verify 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 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 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 are received from industry-accepted time sources.	**10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that the time servers accept time updates from specific, industry-accepted external sources. 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		

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 with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that only 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 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. 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		

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that current audit trail files are promptly backed up to a centralized log server that is difficult to alter. 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		

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, authorization, and accounting protocol (AAA) servers (for example, RADIUS). **Note:** Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.	N/A – Policies and Procedures is the responsibility of the merchant / service provider.		
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that log aggregation solutions generate events and alerts which are reviewed daily.		

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	N/A – Security Policy (Data Retention) is the responsibility of the merchant / service provider.		
	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. **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.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.		

	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 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		
	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.		

	11.1.d If automated monitoring is utilized (for example, wireless IDS/, NAC, etc.), verify the configuration will generate alerts to personnel.	Verizon Business verified If automated monitoring is utilized, the configuration will generate alerts to personnel. 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 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		
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component Installations, changes in network topology, firewall rule modifications, product upgrades). **Note:** It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented	**11.2** Verify that internal and external vulnerability scans are performed as follows:			
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.	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 (not required to be a QSA	N/A – Internal quarterly scanning is the responsibility of the merchant / service provider.		

11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		

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: 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.	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.		
	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.	N/A – Penetration Testing is the responsibility of the merchant / service provider.		
	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.		
	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 intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored. 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 Intrusion Detection Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		
	11.4.b Confirm IDS and/or are configured to alert personnel of suspected compromises.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that they are configured to alert personnel of suspected compromises.		
	11.4.c Examine IDS/ configurations and confirm IDS/ devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that they are configured, maintained, and updated per vendor instructions to ensure optimal protection.		

11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: System executables Application executables Configuration and parameter files Centrally stored, historical or archived, log and audit files	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture for Retail Solutions environment and verified that file-integrity monitoring tools are used.		
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture for Retail Solutions environment and verified that FIM is to be configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly by 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 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company- approved products.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote- access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	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 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4** Verify that information security policies clearly define information security responsibilities for all personnel.	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	N/A – Security Policy is the responsibility of the merchant / service provider.		

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 upon hire and at least annually.	N/A – Security Policy (Security Awareness) is the 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.) **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.	N/A – Security Policy (Background Checks) is the responsibility of the merchant / service provider.		
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 Coverage and responses of all critical system components Reference or inclusion of incident response procedures from the payment brands	**12.9.1.a** Verify that the incident response plan includes: -Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum: Specific incident response procedures Business recovery and continuity procedures Data back-up processes Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) Coverage and responses for all critical system components Reference or inclusion of incident response procedures from the payment brands	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		

	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.		