

# Verizon Business Assessment for: Cisco PCI Solution for Retail: Cisco Systems, Inc.

---

	<b>Based on PCI DSS v. 1.2</b>
	<b>Report Version 1.0</b>
	<b>01/27/2009</b>


## Table of Contents

Contact Information	3
1. Executive Summary	3
Assessment Description	3
Processors Used	4
Connections to Payment Card Companies	4
High Level Network Diagram	5
Quarterly Vulnerability Scans	5
2. Description of Scope of Work and Approach Taken	5
PCI DSS Version	5
Timeframe	6
Locations Visited	6
Environment on which Assessment Focused	6
Network Segmentation	10
Exclusions	11

---

- Wholly-Owned Entities 11
- International Entities 11
- Wireless LANs and/or Wireless Applications 11
- 3. Details about Reviewed Environment 11
  - Description of Cardholder Data Environment 11
  - List of Hardware and Critical Software in Use in the Cardholder Environment 12
  - List of Service Providers 13
  - List of Third-Party Payment Application Products 13
  - List of Individuals Interviewed 13
  - List of Documents Reviewed 14
  - Build and Maintain a Secure Network 15
    - Requirement 1: Install and maintain a firewall configuration to protect cardholder data 15
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 21
  - Protect Cardholder Data 28
    - Requirement 3: Protect stored cardholder data 28
    - Requirement 4: Encrypt transmission of cardholder data across open, public networks 43
  - Maintain a Vulnerability Management Program 45
    - Requirement 5: Use and regularly update anti-virus software or programs 45
    - Requirement 6: Develop and maintain secure systems and applications 48
  - Implement Strong Access Control Measures 58
    - Requirement 7: Restrict access to cardholder data by business need to know 58
    - Requirement 8: Assign a unique ID to each person with computer access. 62
    - Requirement 9: Restrict physical access to cardholder data. 79
  - Regularly Monitor and Test Networks 84
    - Requirement 10: Track and monitor all access to network resources and cardholder data. 84
    - Requirement 11: Regularly test security systems and processes. 97
  - Maintain an Information Security Policy 102
    - Requirement 12: Maintain a policy that addresses information security for employees and contractors. 102

# Contact Information

<p><b>Verizon Business - Security Solutions Powered by Cybertrust</b></p> <p>Aaron Reynolds Sr. Security Consultant CISSP, PCI QSA</p> <p><a href="mailto:aaron.reynolds@verizonbusiness.com">aaron.reynolds@verizonbusiness.com</a> 425.239.2284 (Cell)</p>	
<p><b>Cisco Customer contact information</b></p>	<p><b>Customer logo</b></p>

## 1. Executive Summary

### Assessment Description

Cisco Systems, Inc engaged Verizon Business to conduct a PCI assessment of their “PCI Solution for Retail” architecture, based on the PCI DSS v1.1 standard. The assessment against the PCI DSS v1.1 standard was broken into two phases, which included an initial assessment of the Cisco PCI Solution for Retail network architecture, configurations, security applications, and web consoles, and third-party POS and infrastructure applications. The second phase expanded the scope of the PCI Solution for Retail environment to include review of “at rest” data, remote connectivity solutions, Internet Edge infrastructure, Cisco’s ACE XML firewall, additional network security compliance applications, and review of updated system component versions. The latest phase (phase 3) of the assessment did not include an onsite visit or updated versioning review, with exception to updates to the Cisco ACS software, which fixed a number of password/lockout setting capabilities within Section 8 of the PCI DSS. The focus of phase 3 was to map the previously assessed environment (assessed in August, 2007 – December 2007) against the PCI DSS v1.2 standard. This report captures the results of the v1.2 PCI DSS mapping.

Cisco Systems, Inc will continue to market the assessed 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 (see “Scope” section), targeted to small, medium, and large retail environments. Verizon Business found the three solution architectures to directly address several technical PCI requirements, and can address other requirements either as a compensating control, or in conjunction with compensating controls. 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, mainframes, and corporate networks) were not included in the scope of the assessment.

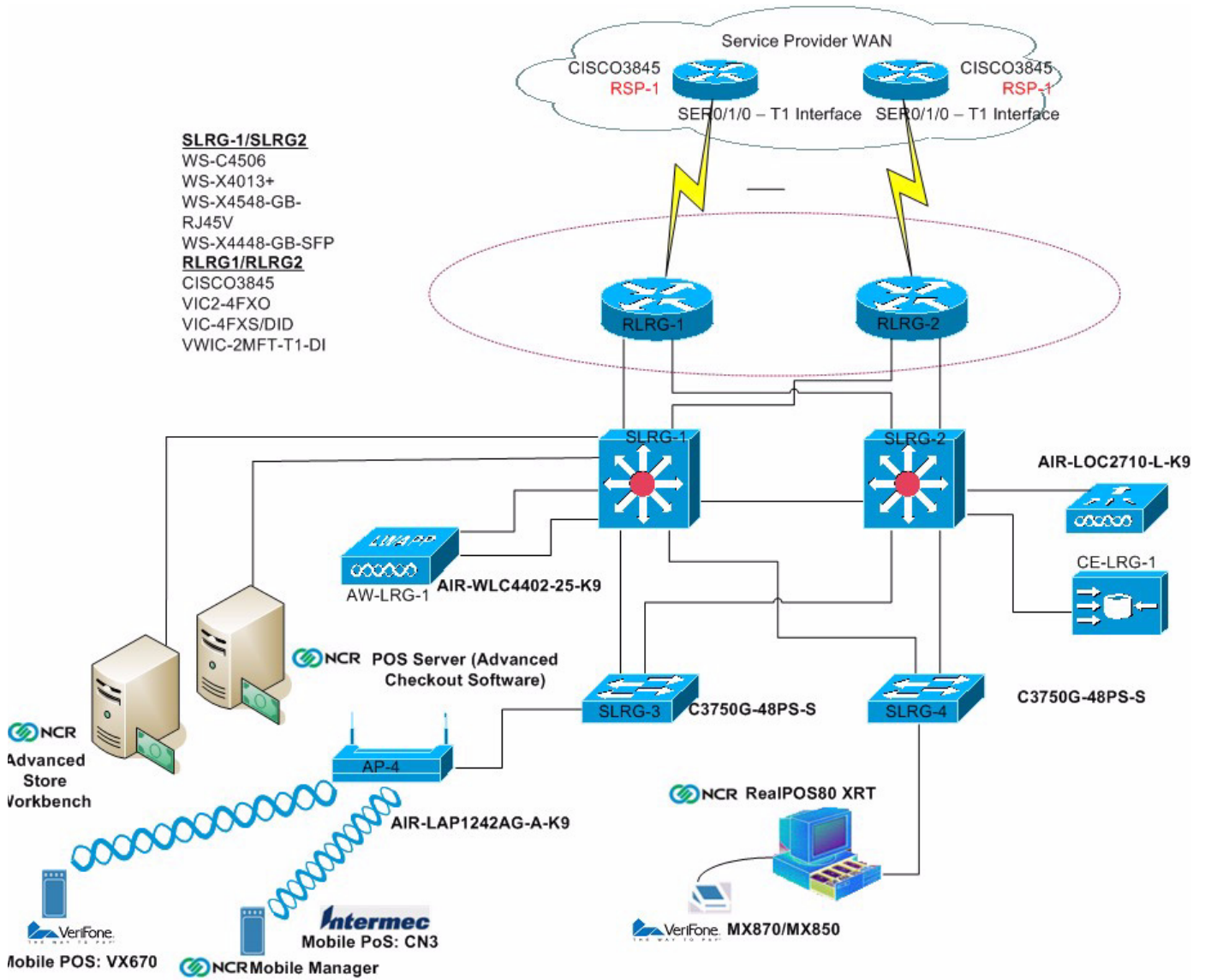
## Processors Used

The assessment took place within Cisco's PCI lab. There were no online transactions or processors involved with the assessment.

## Connections to Payment Card Companies

There were no connections to payment card companies from the Cisco PCI lab.

## 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.1.2 was used for this assessment.

## Timeframe

The assessment took place through several remote interviews, onsite and remote validation during the following two phases:

- Phase 1: 11/16/2006 – 12/29/2006
- Phase 2: 8/24/2007 – 12/12/2007
- Phase 3: 12/28/2008 – 01/26/2009

## Locations Visited

The following Cisco Systems, Inc. locations were visited:

- Cisco Systems, Inc. – PCI Lab (Building J, 255 W. Tasman Drive, San Jose, CA)

## Environment on which Assessment Focused

The assessment included the following “in scope” components:

- Large Retail environment
  - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity): Managed by CSA Manager from Data Center environment.
  - Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
  - Cisco switches – (4 – 2 layer 3 switches (Catalyst 4506), 2 layer 2 access switches (Catalyst 3750))
  - Wireless controllers – (1): Used to monitor and update wireless APs.
  - Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
  - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
  - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
  - Intermec POS: Wireless POS handheld.
  - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.
  - RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.
- Medium Retail environment
  - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)

- Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
  - Cisco 3560 layer 2 switches – (2)
  - Wireless APs – (1) : Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
  - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
  - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
  - Intermec POS: Wireless POS handheld.
  - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.
  - RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.
- Small Retail environment
    - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
    - Cisco 2821 Integrated Services Router (ISR) – (1) – ISR is configured with Firewall and IDS/IPS feature set.
    - Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
    - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
    - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
    - Intermec POS: Wireless POS handheld.
    - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.
    - RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.
  - Data Center Environment
    - Cisco Wireless Control System (WCS): Central platform for wireless configuration, management, and monitoring.

- Cisco Security Monitoring, Analysis and Response System (CS-MARS): Central log monitoring, correlation, and reporting platform for Cisco network device security alerts (e.g. ASA/FWSM/ISR firewall logs and IDS/IPS alerts) within the Large, Medium, and Small retail environments, as well as the data center environment. In addition, Cisco Security Agent alerts are forwarded to CS-MARS.
- CiscoWorks LAN Management Solution (LMS): Network device configuration management (e.g. routing and switching)
- CiscoWorks Network Compliance Manager (NCM): CiscoWorks NCM tracks and regulates configuration and software changes across network infrastructure within the retail store and data center environments. Changes to network device configurations (e.g. enabling telnet, disabling exec timeout, enabling default usernames) are audited and reported through CiscoWorks NCM.
- Cisco Security Manager (CSM): Central provisioning of device configuration and security policies, including: ASAs, FWSMs, IDS/IPS, ISRs and switches (e.g. firewall policy, IDS/IPS configuration and signature management, https access).
- Cisco Security Agent (CSA) Manager – CSA software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
- Cisco Secure Access Control Server (ACS) – AAA server
- Cisco Application Control Engine (ACE – XML Gateway): Although initially designed for XML and SOAP-based web services, ACE XML Gateway demonstrated capabilities to provide application layer defense against html-based web vulnerabilities and attacks. ACE XML Gateway was deployed in the Internet Edge (DMZ) segment of the data center environment.
- Cisco Adaptive Security Device Manager (ASDM): Secure, web-based configuration management of ASA firewalls.
- Cisco IPS Device Manager (IDM): IDS/IPS configuration management.
- Cisco Security Device Manager (SDM): Secure, web-based configuration management of 7206VXR routers.
- Cisco 7206 VXR router (2 at Internet Edge, 2 at WAN aggregation): Access lists, routing, IPSec VPN termination.
- Cisco Catalyst 3750 switch (6 – 2 Internet Edge, 4 WAN aggregation): Layer 3 switch (routing and access lists).
- Cisco Catalyst 6509 Switch (8 – 2 Internet Edge, 2 core datacenter switch, 2 service aggregation switch, 2 access switch): Internet Edge – Routing, FWSM, IDSM2, and Application Control Engine (ACE – load balancer) modules, Core datacenter – layer 3 switch (routing and access lists), core service aggregation – layer 3 switch (routing, access lists, and IDSM module)
- Cisco Catalyst 4948 Switch (2): Layer 2 access switch.
- Cisco Adaptive Security Appliance (ASA) 5540 (2): Stateful firewall filtering and integrated IDS/IPS @ data center boundary.
- RSA File Security Manager: Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server (within retail store environment) and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server. This was a small demonstration of RSA File Security Manager's capabilities to transparently encrypt/decrypt data using strong AES and/or 3DES encryption. The configuration of RSA File Security Manager within the assessed environment was found to meet all key management requirements under PCI DSS v1.1.



- RSA Key Manager: Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information. RSA Key Manager is the central platform to manage security policies for encryption and decryption of data. The configuration of RSA Key Manager within the assessed environment was found to meet all key management requirements under PCI DSS v1.1.
- RSA Access Manager: Used for central authentication/logging for access to RSA Key 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 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.

The following system components were part of the sample:

Component	Brand(s) Used	Version
Firewall	<ul style="list-style-type: none"> <li>• Cisco Integrated Services Router (FWSM Firewall), Cisco ASA</li> </ul>	<ul style="list-style-type: none"> <li>• FWSM v3.1(3)</li> <li>• ASA 7.2.(2)</li> </ul>
Network IDS	Cisco Integrated Services Router (integrated IDS/IPS), IDSM2	IOS v12.3(11r)T2, 12.4(1r), IDSM 6.0.(2)E1
Router	Cisco Integrated Services Router (IOS Firewall), Cisco 7206VXR	IOS v12.2(18)SXF10a, v12.3(11r)T2, 12.4(1r), 12.4(11)T3 (VXR)
Wireless AP	Cisco 1131AG, 1242AG	
Wireless Controller	AIR-LAP1131AG-A-K9, AIR-LAP1242AG-A-K9	IOS 12.3(11)JA
POS Software	NCR ACS, NCR RealPOS	ACS v6.01.04.16
POS Devices	NCR, Verifone, Intermec	NCR RealPOS 80c, Verifone MX870, MX850, Vx670 (wireless), and Intermec Mobile POS CN3 (wireless)
Windows Server	Windows Server 2003	SP1, SP2
ECOM Web Server (demo server)	Foundstone Hackme Bank	v2.0
Database	N/A – Not reviewed/Not in scope	
Windows Server Anti-Virus	McAfee VirusScan Enterprise + Anti-spyware Module	8.0.0
Firewall, Router, Switch, IDS/IPS Management	Cisco Security Manager (CSM), Cisco ASDM, Cisco IDM	CSM v3.0.1, ASDM v5.2.(2), IDM v6.0.2
Router, Switch management	CiscoWorks (LMS), CiscoWorks (NCM)	LMS v2.6, NCM v1.2.1
Desktop/Server Firewall (Host-based firewall)	Cisco Security Agent (CSA)	v5.1.0.69, v5.2.0.210
Central Logging / Correlation /Analysis	CS-MARS, RSA enVision	CS-MARS (v4.3.1), enVision (v3.5.1)
Wireless Management	Wireless Control System (WCS)	v4.1
AAA (TACACS+) authentication	Cisco ACS	v4.1(3) Build 12
Web Services (application) firewall	Cisco ACE XML Gateway	V5

Load Balancer	Cisco ACE Load Balancer	V3.0(0)A1(4a)
Two-factor Authentication	RSA SecurID (RSA Authentication Manager)	V6.1(300)
RSA Key Manager Authentication	RSA Access Manager	v6.0
Desktop E-mail Encryption	N/A – not in scope	
File Integrity	Cisco Security Agent (CSA)	v5.1
Cardholder Storage Encryption	<ul style="list-style-type: none"> <li>• NCR ACS (128-bit 3DES)</li> <li>• RSA Key Manager (192-bit 3DES, 128-bit, 192-bit, 256-bit AES)</li> <li>• RSA File Security Manager (192-bit 3DES, 256-bit AES)</li> </ul>	<ul style="list-style-type: none"> <li>• ACS v6.01.04.16</li> <li>• RSA Key Manager v2.1.1</li> <li>• RSA File Security Manager v2.1.0.9</li> </ul>

## 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/IPS, and routing functionality. Extremely explicit access-lists are applied through CSM 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 port level. Additionally, Cisco has incorporated wireless into the design, using WPA-TKIP w/PEAP 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.

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 FWSM and ASA stateful firewall filtering, IDSM and integrated IDS/IPS detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication using RSA SecurID tokens.

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/IPS signatures))
- CiscoWorks LAN Management Solution (LMS) – (Central configuration management for ISRs and switches (e.g. routing, switching, VLANs))
- CiscoWorks Network Compliance Manager (NCM) – (Central platform for auditing changes and enforcing configuration standards across network devices within the environment.
- Cisco Wireless Control System (WCS) – (Central wireless management)
- Cisco Security Agent (CSA) Manager – (Central CSA software manager: HIDS, Host-based firewall, file monitoring / Access Control, Malware protection, zero-day, behavioral A/V protection)
- Cisco ACS – (Central TACACS+ (central authentication) server for ASA firewall, FWSM, ISR, 7206 VXR router, switch, wireless controller, CiscoWorks (LMS and NCM), CS-MARS, WCS, and CSM).
- CS-MARS – (Central logging / Correlation / Analysis / Alerting server. Alerts from IDS/IPS alerts, CSA alerts, firewall logs)
- Cisco ASDM – (Central configuration for ASA firewalls).
- Cisco IPS Device Manager (IDM): IDS/IPS configuration management.
- Cisco Security Device Manager (SDM): Secure, web-based configuration management of 7206VXR routers.

## Exclusions

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

- Central cardholder data storage (limited to central storage on secure file repository, using RSA File Security Manager for data encryption)
- Authorization / Settlement processes
- Policies, procedures, and standards
- Assessment of “in transit” cardholder data (limited to transmission of test files between large store and data center using SCP to securely transmit file from back-office POS system (NCR ACS server) to secure file repository in data center environment)
- OS security for WCS, CS-MARS, CiscoWorks (LMS), CSM, CSA Manager, Cisco ACS, RSA enVision, RSA Key Manager, RSA File Security Manager, NCR Advanced Checkout Solution (ACS), RSA Authentication Manager, RSA Access Manager, Cisco Network Compliance Manager (NCM),
- Physical Security
- SDLC policies and procedures
- Live cardholder transactions (A fully functional POS environment, which includes authorization responses, was not available during the assessment)

## Wholly-Owned Entities

N/A – There were no wholly-owned entities involved in the assessment.

## International Entities

N/A – There were no international entities involved in the assessment.

## Wireless LANs and/or Wireless Applications

Wireless networks within the PCI Solution for Retail environment have been configured to use WPA-TKIP w/PEAP 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, SSID broadcast disabled, default SSID has been changed, SNMPv3 used (default strings changed), and http access has been disabled.

# 3. Details about Reviewed Environment

## Description of Cardholder Data Environment

NCR Advanced Checkout Solution (ACS) POS software was used within the Cisco Solution for Retail environment. NCR ACS software has been successfully certified through the Payment Application Best Practice (PABP) certification process. NCR ACS software handles both online and offline cardholder transactions, including debit and credit transactions. NCR ACS software protects “at rest” cardholder data through 3DES encryption, truncation, and masking, including for offline transactions.

## List of Hardware and Critical Software in Use in the Cardholder Environment

The following hardware and software are critical for the cardholder environment:

Component	Brand(s) Used	Version
Firewall	<ul style="list-style-type: none"> <li>Cisco Integrated Services Router (FWSM Firewall), Cisco ASA</li> </ul>	<ul style="list-style-type: none"> <li>FWSM v3.1(3)</li> <li>ASA 7.2.(2)</li> </ul>
Network IDS	Cisco Integrated Services Router (integrated IDS/IPS), IDSM2	IOS v12.3(11r)T2, 12.4(1r), IDSM 6.0.(2)E1
Router	Cisco Integrated Services Router (IOS Firewall), Cisco 7206VXR	IOS v12.2(18)SXF10a, v12.3(11r)T2, 12.4(1r), 12.4(11)T3 (VXR)
Wireless AP	Cisco 1131AG, 1242AG	
Wireless Controller	AIR-LAP1131AG-A-K9, AIR-LAP1242AG-A-K9	IOS 12.3(11)JA
POS Software	NCR ACS, NCR RealPOS	ACS v6.01.04.16
POS Devices	NCR, Verifone, Intermec	NCR RealPOS 80c, Verifone MX870, MX850, Vx670 (wireless), and Intermec Mobile POS CN3 (wireless)
Windows Server	Windows Server 2003	SP1, SP2
ECOM Web Server (demo server)	Foundstone Hackme Bank	v2.0
Database	N/A – Not reviewed/Not in scope	
Windows Server Anti-Virus	McAfee VirusScan Enterprise + Anti-spyware Module	8.0.0
Firewall, Router, Switch, IDS/IPS Management	Cisco Security Manager (CSM), Cisco ASDM, Cisco IDM	CSM v3.0.1, ASDM v5.2.(2), IDM v6.0.2
Router, Switch management	CiscoWorks (LMS), CiscoWorks (NCM)	LMS v2.6, NCM v1.2.1
Desktop/Server Firewall (Host-based firewall)	Cisco Security Agent (CSA)	v5.1.0.69, v5.2.0.210
Central Logging / Correlation /Analysis	CS-MARS, RSA enVision	CS-MARS (v4.3.1), enVision (v3.5.1)
Wireless Management	Wireless Control System (WCS)	v4.1
AAA (TACACS+) authentication	Cisco ACS	v4.0(1) Build 27
Web Services (application) firewall	Cisco ACE XML Gateway	V5
Load Balancer	Cisco ACE Load Balancer	V3.0(0)A1(4a)
Two-factor Authentication	RSA SecurID (RSA Authentication Manager)	V6.1(300)
RSA Key Manager Authentication	RSA Access Manager	v6.0
Desktop E-mail Encryption	N/A – not in scope	

File Integrity	Cisco Security Agent (CSA)	v5.1
Cardholder Storage Encryption	<ul style="list-style-type: none"> <li>NCR ACS (128-bit 3DES)</li> <li>RSA Key Manager (192-bit 3DES, 128-bit, 192-bit, 256-bit AES)</li> <li>RSA File Security Manager (192-bit 3DES, 256-bit AES)</li> </ul>	<ul style="list-style-type: none"> <li>ACS v6.01.04.16</li> <li>RSA Key Manager v2.1.1</li> <li>RSA File Security Manager v2.1.0.9</li> </ul>

## List of Service Providers

There were no Service Providers that were included in the assessment.

## List of Third-Party Payment Application Products

NCR Advanced Checkout Solution (ACS) POS software was used within the Cisco Solution for Retail environment. NCR ACS software has been successfully certified through the Payment Application Best Practice (PABP) certification process. NCR ACS software handles both online and offline cardholder transactions, including debit and credit transactions. NCR ACS software protects “at rest” cardholder data through 3DES encryption, truncation, and masking, including for offline transactions.

## List of Individuals Interviewed

The following staff was interviewed:

Interviewee(s)	Title	Date
Christian Janoff, Bart Mcglothin, Chris Tobkin, Stephan, Christina Hausman, Josh Huston	Environment Overview, Cisco PCI designs (CS-MARS, CSA, CSM, CiscoWorks (LMS), ACS, WCS)	11/16/06
Christian Janoff, Bart Mcglothin, Chris Tobkin, Stephan, Christina Hausman, Josh Huston	Environment Overview, Cisco PCI designs (CS-MARS, CSA, CSM, CiscoWorks (LMS), ACS, WCS)	11/17/06
Christian Janoff, Bart Mcglothin	Network architecture, firewalls, routers, switches, wireless, IDS/IPS	12/04/06
Christian Janoff, Bart Mcglothin	Audit Logging	12/04/06
Christian Janoff, Bart Mcglothin	Access Control / Authentication	12/04/06
Christian Janoff, Bart Mcglothin	CSA	12/04/06
Christian Janoff, Bart Mcglothin	MARS	12/04/06
Christian Janoff, Bart Mcglothin	CSM	12/04/06
Christian Janoff, Bart Mcglothin	Wireless	12/04/06
Christian Janoff, Bart Mcglothin	CiscoWorks (LMS)	12/06/06
Christian Janoff, Bart Mcglothin, Eric	MARS	12/13/06
Christian Janoff, Bart Mcglothin	Remediation items	12/20/06
Christian Janoff, Bart Mcglothin, Paul Jones	Assessment Results – Messaging	12/21/06
Christian Janoff, Bart Mcglothin, Christina Hausman, Josh Huston	CSA validation	12/22/06
Christian Janoff, Bart Mcglothin	IRoC review, remediation, and clarifications	12/27/06
Rupesh Chakkingal, Karen Chan	Cisco Retail Solution (Phase II overview)	9/13/07

Karen Chan, Sam Rao	CiscoWorks NCM	9/21/07
Karen Chan	Datacenter topology (WAN aggregation, DMZ, Internet Edge)	10/2/07
Karen Chan, Edmond Lam	7206VXR configuration review	10/4/07
Rupesh Chakkingal, Prakash Sinha	ACE XML Gateway	10/9/07
Rupesh Chakkingal, Scot Delancey (NCR)	NCR ACS Server	10/9/07
Rupesh Chakkingal, Ken Moore (Verifone), Marco (Verifone), Dave (Verifone)	Verifone MX/VX Series Pin Pads	10/9/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager	10/10/07
Rupesh Chakkingal, Mohan Atreya (RSA)	RSA File Security Manager	10/10/07
Karen Chan, Don Lanoue, Mark King, Scott Seal	Cisco Configuration Assurance Solution (CAS)	10/11/07
Karen Chan	Cisco Network Compliance Manager (NCM)	10/15/07
Karen Chan	Data Center Network review	10/15/07
Rupesh Chakkingal, Mohan Atreya (RSA)	RSA File Security Manager	10/15/07
Karen Chan	Cisco router secure configuration reviews	10/16/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager	10/16/07
Karen Chan, Pete Davis, Sridharan Srinivasan	Cisco ASA – Secure configuration reviews	10/17/07
Rupesh Chakkingal, Bryan Finch (NCR), Scot Delancey (NCR)	NCR ACS Server (Encryption/Key Management, Retention, password/lockout security, least-privilege access)	10/17/07
Rupesh Chakkingal, Chris Paggen	Cisco ACE XML Gateway (Web application security)	10/17/07
Karen Chan	VSAN Storage (EMC Storage) security – Zoning/LUN Masking	11/19/07
Rupesh Chakkingal, Josh Huston, John Eppich	Cisco Security Agent	11/19/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA File Security Manager	11/19/07
Rupesh Chakkingal, Joe Vittorioso (RSA), Duke Corey (RSA)	RSA enVision	12/6/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Authentication Manager, RSA SecurID	12/6/07
Rupesh Chakkingal, Martin Pueblas	Cisco IDSM review	12/6/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager, RSA Access Manager, RSA Authentication Manager	12/7/07
Rupesh Chakkingal, David Paschich	Cisco ACE XML Gateway (web application security)	12/7/07
Karen Chan	VSAN Storage – Security review	12/7/07

## List of Documents Reviewed

The following documents were interviewed:

Document	Version / Date
LAB Servers and PC's V12 2006-12-27.doc	12/26/07 / v13
NTPVMapp_FAQ.txt	12/27/06
PCI Lab Application Flows v6 2006-12-27.xls	12/27/06
PCI LAB DOC DIAGRAMS 2006-12.01.vsd	12/01/06
Cisco Retail PCI Lab 11.20.06.doc	11/20/06

Cisco Security Agent v5.1 Test Guide.pdf	2006
CSA for corporate clients.pdf	
CSA deployment best practices.pdf	
Firewall Documentation.doc	11/16/06
PCI DIG v3. 12.19.06.doc	12/19/06

## Build and Maintain a Secure Network

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

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

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, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection 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.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
<b>1.1</b> Establish firewall and router configuration standards that include the following:	<b>1.1</b> Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
<b>1.1.1A</b> formal process for approving and testing all network connections and changes to the firewall and router configurations	<b>1.1.1</b> 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).		<a href="#">Responsibility of merchant / service provider.</a>

### 3. Details about Reviewed Environment

<p><b>1.1.2</b>Current network diagram with all connections to cardholder data, including any wireless networks</p>	<p><b>1.1.2.a</b> 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.</p>	<p>Cisco provided a current network diagram, which documents all connections to the cardholder data, applicable to the reference architecture environment, including wireless networks.</p>		
	<p><b>1.1.2.b</b> Verify that the diagram is kept current.</p>	<p>Current diagrams were provided for each PCI Solution for Retail environment (e.g. Small, medium, and large POS environments, and data center environment).</p>		<p><b>Note:</b> Since each network environment will be unique to the merchant or service provider, updating network diagrams remains the responsibility of each merchant / service provider.</p>
<p><b>1.1.3</b>Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</p>	<p><b>1.1.3</b>Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>
<p><b>1.1.4</b>Description of groups, roles, and responsibilities for logical management of network components</p>	<p><b>1.1.4</b>Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p> <p><b>Note:</b> 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).</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>



<p><b>1.1.5</b> 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</p>	<p><b>1.1.5.a</b> 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.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p> <p><b>Note:</b> 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.</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>
	<p><b>1.1.5.b</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. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>
<p><b>1.1.6</b> Requirement to review firewall and router rule sets at least every six months</p>	<p><b>1.1.6.a</b> Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p>		<p>Responsibility of merchant / service provider.</p>
	<p><b>1.1.6.b</b> Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p>		<p>Responsibility of merchant / service provider.</p> <p><b>Note:</b> Requirement to review rule sets is to identify and remove stale, unnecessary rules, as well as audit rule set for soundness against current network design.</p>
<p><b>1.2</b> Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.</p> <p>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.</p>	<p><b>1.2</b> Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:</p>			

### 3. Details about Reviewed Environment

<p><b>1.2.1</b> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.</p>	<p><b>1.2.1.a</b> Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.</p>	<p>Verizon Business confirmed that inbound traffic to and outbound traffic from the PCI Solution for Retail environment is limited to protocols necessary for the environment. ASA firewalls, FWSM firewalls, Integrated Services Routers (ISRs), and router access-lists are configured with “default-deny” rules and explicitly allow traffic to the service/port level.</p>		<p><a href="#">Configurations for perimeter firewalls/routers outside the PCI Solution for Retail environment are the responsibility of merchant / service provider.</a></p>
	<p><b>1.2.1.b</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.</p>	<p>Verizon Business confirmed that all inbound and outbound traffic not necessary for the PCI Solution for Retail environment is specifically denied.</p>		
<p><b>1.2.2</b> Secure and synchronize router configuration files.</p>	<p><b>1.2.2</b> 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.</p>	<p>Verizon Business confirmed Cisco ISR and Cisco router device configurations are stored locally and within CiscoWorks (LMS, NCM), which has been implemented with least privilege access. CiscoWorks (LMS, NCM) can be configured to log and alert on configuration inconsistencies between active (running) and startup configurations.</p>		
<p><b>1.2.3</b> 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.</p>	<p><b>1.2.3</b> 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.</p>	<p>Verizon Business confirmed the PCI Solution for Retail environment architecture was designed and segmented to require all wireless traffic destined for any wired host (e.g. POS system, WCS Manager, etc.) to pass through ISR firewall access-lists before being permitted.</p>		
<p><b>1.3</b> Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p>	<p><b>1.3</b> Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.</p>			

<b>1.3.1</b> Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	<b>1.3.1</b> Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	Verizon Business reviewed access-lists for inbound and outbound Internet traffic and confirmed traffic is limited to only protocols that are necessary for the cardholder data environment.		
<b>1.3.2</b> Limit inbound Internet traffic to IP addresses within the DMZ.	<b>1.3.2</b> Verify that inbound Internet traffic is limited to IP addresses within the DMZ.	Verizon Business reviewed access-lists for inbound Internet traffic and confirmed traffic is limited to IP addresses within the DMZ and restricted to only those services/protocols necessary.		Perimeter firewall/router configurations and rule sets are the responsibility of the merchant / service provider.
<b>1.3.3</b> Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	<b>1.3.3</b> Verify there is no direct route inbound or outbound 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 confirmed there are no direct routes inbound or outbound for Internet traffic to/from the retail reference architecture.		Merchant / Service Provider would be responsible for ensuring POS devices and other servers in the retail (POS) environment are not configured to communicate directly with the Internet.
<b>1.3.4</b> Do not allow internal addresses to pass from the Internet into the DMZ.	<b>1.3.4</b> 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.		
<b>1.3.5</b> Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	<b>1.3.5</b> Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.	Verizon Business reviewed outbound access-lists from the PCI Solution for Retail environment and confirmed that all outbound traffic is destined for “data center” systems. There is no outbound Internet access from the PCI Solution for Retail environment.		

### 3. Details about Reviewed Environment

<p><b>1.3.6</b> Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)</p>	<p><b>1.3.6</b> 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 (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set—a response means packets are allowed through even if they are not part of a previously established session).]</p>	<p>Verizon Business confirmed the PCI Solution for Retail environment configurations for the Cisco ASA firewalls, FWSMs, and ISRs were configured to perform stateful packet inspections.</p>		
<p><b>1.3.7</b> Place the database in an internal network zone, segregated from the DMZ.</p>	<p><b>1.3.7</b> Verify that the database is on an internal network zone, segregated from the DMZ.</p>	<p>All databases within the PCI Solution for Retail environment are on an internal segment, segregated from the DMZ.</p>		
<p><b>1.3.8</b> Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).</p>	<p><b>1.3.8</b> For the sample of firewall and router components, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).</p>	<p>Verizon Business reviewed DHCP reservations, static IPs, and access lists across firewalls and routers and confirmed RFC 1918 addresses were used within the PCI Solution for Retail environment.</p>		
<p><b>1.4</b> 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.</p>	<p><b>1.4.a</b> 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.</p>	<p>N/A – Security Policy (Remote Access – Desktop firewalls)</p> <p><b>Note:</b> Remote access to the PCI Solution for Retail environment was assessed for two-factor authentication (requirement 8.3) only.</p>		<p>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.</p>
	<p><b>1.4.b</b> Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.</p>	<p>See 1.4.a above.</p>		<p>See 1.4.a above.</p>

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

Malicious individuals (external and internal to a company) 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	Target Date/ Comments
2.1 Always change vendor-supplied defaults <b>before</b> installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	2.1 Choose a sample of system components, critical servers, and wireless access points, 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.		

<p><b>2.1.1</b>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. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.</p>	<p><b>2.1.1</b> Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES):</p> <p>Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions</p> <p>Default SNMP community strings on wireless devices were changed</p> <p>Default passwords/passphrases on access points were changed</p> <p>Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)</p> <p>Other security-related wireless vendor defaults, if applicable</p>	<p>Verizon Business reviewed wireless settings within the PCI Solution for Retail environment and verified the following:</p> <ul style="list-style-type: none"> <li>- Although default configurations support WEP, WEP keys had been disabled and were not used within the wireless environment. WPA/TKIP (w/PEAP authentication) is used for all wireless security.</li> <li>- No Default SSID exists. This must be entered at initial installation, and is recommended by Cisco to be unique.</li> <li>- SSID broadcast was disabled.</li> <li>- Default SNMP community strings have been changed and (SNMPv3 is being used).</li> <li>- 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 environment.</li> <li>- WPA technology is enabled (WPA/TKIP w/PEAP authentication).</li> <li>- Wireless management and web mode is disabled.</li> </ul>		
--	--	--	--	--

<p><b>2.2</b>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.</p>	<p><b>2.2.a</b>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—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p><b>Note:</b> Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards. CiscoWorks NCM can be used to further support best practice standards across network devices. Network device templates can be created to standardize secure configurations across network devices. Additionally, NCM can be used to periodically (e.g. once a day) audit network configurations to ensure secure configurations are being used and have not been altered contrary to best-practice standards.</p> <p><b>Note:</b> Host Operating Systems were not included in the secure configuration review, as the OS chosen for management applications could vary with each merchant/service provider. Secure configuration for chosen OS platforms would be performed by the merchant/service provider. Verizon Business reviewed administrative accounts (default username/passwords, password/lockout settings, audit log settings, and secure channels for administration of applications and systems.</p>	<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>
	<p><b>2.2.b</b>Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4).</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p><b>Note:</b> Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards.</p>	<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>

	<p><b>2.2.c</b> Verify that system configuration standards are applied when new systems are configured.</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p><b>Note:</b> Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards. Verizon Business also confirmed all management consoles were configured to support https access, and that http access had been disabled.</p>		<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>
<p><b>2.2.1</b> Implement only one primary function per server.</p>	<p><b>2.2.1</b> For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Within the PCI Solution for Retail environment Cisco has used Virtual (VMware) servers to logically segment system functionality within a single hardware device (e.g. CSA Manager and CSM (Cisco Security Manager) running under separate VMware servers on a single system.</p>		<p><b>Note:</b> Logical system partitioning (e.g. lpars (IBM mainframe), VMware servers) is an acceptable means to separate server functions within a single server platform.</p>



<p><b>2.2.2</b> Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).</p>	<p><b>2.2.2</b> For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.</p>	<p>Verizon Business reviewed configurations for ASA/FWSM firewalls, ISR routers, switches, and wireless devices and found insecure services and protocols to be disabled.</p> <p><b>Note:</b> Although Cisco followed a configuration standard to harden the OS for management consoles and POS servers (e.g. WCS, ACS, CSM, CSA, CiscoWorks (LMS, NCM), ACE XML Gateway, RSA File Security Manager, RSA Key Manager, RSA Access Manager, RSA Authentication Manager, and RSA enVision), 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.</p>		<p>Host OS hardening for POS applications, Management servers (e.g. Cisco CSM, RSA Authentication Manager, etc) is the responsibility of the merchant/service provider.</p>
<p><b>2.2.3</b> Configure system security parameters to prevent misuse.</p>	<p><b>2.2.3.a</b> Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.</p>	<p>Verizon Business interviewed administrators, architects, and SMEs from business units to determine they have knowledge of common security parameters for the ASA firewalls, FWSMs, ISRs, routers, switches, wireless components, and management platforms within the PCI Solution for Retail environment.</p>		<p>Interviews to be conducted within respective administrator/security groups for each merchant / service provider.</p>
	<p><b>2.2.3.b</b> Verify that common security parameter settings are included in the system configuration standards.</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p><b>Note:</b> Verizon Business reviewed configurations across ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were based on best practice standards. 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.</p>		<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>

	<p><b>2.2.3.c</b>For a sample of system components, verify that common security parameters are set appropriately.</p>	<p>Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices 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 network devices (e.g. ASA/FWSM firewalls, ISRs, routers, switches, wireless controllers) and for management of WCS, CSA, CiscoWorks (LMS, NCM), CSM, CS-MARS, and ACS, ACE XML Gateway, NCR ACS server, RSA File Security Manager, RSA Key Manager, RSA enVision, RSA Authentication Manager, and RSA Access Manager.</p>		<p>Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.</p>
<p><b>2.2.4</b>Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.</p>	<p><b>2.2.4</b>For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented and support secure configuration, and that only documented functionality is present on the sampled machines.</p>	<p>Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were based on best practice standards, and that all unnecessary functionality was disabled.</p>		<p>Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.</p>

<p><b>2.3</b>Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</p>	<p><b>2.3</b>For a sample of system components, verify that non-console administrative access is encrypted by:</p> <ul style="list-style-type: none"> <li>• Observing an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested;</li> <li>• Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally; and</li> <li>• Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.</li> </ul>	<p>Verizon Business reviewed non-console administrative access for ASA firewalls, FWSM firewalls, ISR routers, switches, wireless devices, and the following management consoles: CSA Manager, ACS (TACACS+ server for all network device authentication), CSM, CiscoWorks (LMS,NCM), WCS (wireless console), and ACE XML Gateway, CS-MARS, NCR ACS Server, RSA File Security Manager, RSA Key Manager, RSA enVision, RSA Authentication Manager, and RSA Access Manager . Verizon Business confirmed the following methods were used:</p> <ul style="list-style-type: none"> <li>- ssh (CLI access for ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2 modules, ACE XML Gateway, CS-MARS, and wireless controllers)</li> <li>- RDP (High Encryption) enabled. This forces RDP clients to used 128-bit encryption. RDP access is used to for OS access for the following: NCR ACS server, all Windows-based Cisco management consoles (e.g. CiscoWorks (LMS, NCM), WCS, CSA, ACS, etc), RSA File Security Manager, RSA Key Manager, RSA Authentication Manager, RSA Access Manager, RSA enVision.</li> <li>- 128-bit SSL (https) or SSL encrypted thick-client access for management console access, including wireless console access (WCS).</li> <li>- Http access has been disabled on all management consoles, ASA/FWSM firewalls, ISRs, routers, switches, and wireless controllers.</li> </ul>		<p><b>Note:</b> 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.</p>
<p><b>2.4</b>Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in <i>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i>.</p>	<p><b>2.4</b>Perform testing procedures <b>A.1.1</b> through <b>A.1.4</b> detailed in <i>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i> 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.</p>	<p>N/A – Hosting provider (testing procedures) requirement</p>		<p>This requirement is specific to hosting providers.</p>

## 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 network 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 PAN in unencrypted e-mails.

Please refer to the *PCI 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	Target Date/ Comments
<p><b>3.1</b>Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.</p>	<p><b>3.1</b>Obtain and examine the company policies and procedures for data retention and disposal, and perform the following:</p> <ul style="list-style-type: none"> <li>• Verify that policies and procedures 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)</li> <li>• Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data</li> <li>• Verify that policies and procedures include coverage for all storage of cardholder data</li> <li>• Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements</li> </ul>	<p>N/A – Data retention / Data disposal policy and procedures.</p>		<p>Data retention / Data disposal policies and procedures are the responsibility of the merchant / service provider.</p>

<p><b>3.2</b>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:</p>	<p><b>3.2</b>If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable.</p> <p>For each item of sensitive authentication data below, perform the following steps:</p>	<p>VzB observed test transactions and “at rest” data within the NCR POS terminal and NCR ACS application. Verizon Business also reviewed NCR’s PABP assessment results and confirmed that NCR ACS software used within Cisco’s PCI Solution for Retail environment is PABP certified. As a result of the review, Verizon Business has confirmed that sensitive authentication data is not stored subsequent to authorization.</p> <p>Like other POS applications, the NCR ACS software does retain full track data in 128-bit 3DES encrypted format, only in an offline scenario (link to authorizer is down), and is purged at the point the connection is available and the transaction is sent for authorization.</p>	<p>It is the responsibility of the merchant to ensure POS systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted). A large step to ensure POS systems meet PCI requirements is to work with POS vendors that have certified their POS application/s according to PABP standards.</p>
--	--	--	---

<p><b>3.2.1</b> Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><b>Note:</b> In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</p> <ul style="list-style-type: none"> <li>• The cardholder's name,</li> <li>• Primary account number (PAN),</li> <li>• Expiration date, and</li> <li>• Service code</li> </ul> <p>To minimize risk, store only these data elements as needed for business.</p> <p><b>Note:</b> See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</p>	<p><b>3.2.1</b> For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs (for example, transaction, history, debugging, error)</li> <li>• History files</li> <li>• Trace files</li> <li>• Several database schemas</li> <li>• Database contents</li> </ul>	<p>See 3.2 above. Verizon Business confirmed that full track data is not written to disk, other than temporarily in an offline scenario. During this temporary period the track data is encrypted using 128-bit 3DES encryption, and is immediately purged at the point an authorization response is obtained. Verizon Business reviewed the following:</p> <ul style="list-style-type: none"> <li>• Database transaction files</li> <li>• User access log</li> <li>• EFT Journal Report</li> <li>• EFT Offline Report</li> <li>• EFY Rejection Report</li> <li>• Electronic Journal Report</li> <li>• TRMOFF (FOH offline transaction file)</li> <li>• EFTOFF (back office offline transaction file)</li> </ul>	<p><a href="#">See 3.2 above</a></p>
--	--	--	--------------------------------------

<p><b>3.2.2</b> 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.</p> <p><i>Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>	<p><b>3.2.2</b> For a sample of system components, 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:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs (for example, transaction, history, debugging, error)</li> <li>• History files</li> <li>• Trace files</li> <li>• Several database schemas</li> <li>• Database contents</li> </ul>	<p>See 3.2 above. Verizon Business observed that CVV2/CVC2 data was not received at POS swipe. Verizon Business reviewed the following to confirm CVV/CVC2 data is not present:</p> <ul style="list-style-type: none"> <li>• Database transaction files</li> <li>• User access log</li> <li>• EFT Journal Report</li> <li>• EFT Offline Report</li> <li>• EFY Rejection Report</li> <li>• Electronic Journal Report</li> <li>• TRMOFF (FOH offline transaction file)</li> <li>• EFTOFF (back office offline transaction file)</li> </ul>	<p><a href="#">See 3.2 above</a></p>
<p><b>3.2.3</b> Do not store the personal identification number (PIN) or the encrypted PIN block.</p>	<p><b>3.2.3</b> For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs (for example, transaction, history, debugging, error)</li> <li>• History files</li> <li>• Trace files</li> <li>• Several database schemas</li> <li>• Database contents</li> </ul>	<p>See 3.2 above. Verizon Business observed that PIN/PIN block data was not required at POS swipe. Verizon Business reviewed NCR's PABP assessment results and the following to confirm CVV/CVC2 data is not present:</p> <ul style="list-style-type: none"> <li>• Database transaction files</li> <li>• User access log</li> <li>• EFT Journal Report</li> <li>• EFT Offline Report</li> <li>• EFY Rejection Report</li> <li>• Electronic Journal Report</li> <li>• TRMOFF (FOH offline transaction file)</li> <li>• EFTOFF (back office offline transaction file)</li> </ul>	<p><a href="#">See 3.2 above</a></p>




<p><b>3.3</b>Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> <li>• This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.</li> <li>• This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.</li> </ul>	<p><b>3.3</b>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.</p>	<p>Verizon Business reviewed NCR's ACS application and confirmed that only masked data is accessible through the application, even for administrators.</p>		<p>Data control / 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.</p>
---	--	--	--	---

<p><b>3.4</b> Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:</p> <ul style="list-style-type: none"> <li>• One-way hashes based on strong cryptography</li> <li>• Truncation</li> <li>• Index tokens and pads (pads must be securely stored)</li> <li>• Strong cryptography with associated key-management processes and procedures</li> </ul> <p>The MINIMUM account information that must be rendered unreadable is the PAN.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>• If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.</li> <li>• “Strong cryptography” is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.</li> </ul>	<p><b>3.4.a</b> 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 one of the following methods:</p> <ul style="list-style-type: none"> <li>• One-way hashes based on strong cryptography</li> <li>• Truncation</li> <li>• Index tokens and pads, with the pads being securely stored</li> <li>• Strong cryptography, with associated key-management processes and procedures</li> </ul>	<p>Verizon Business reviewed vendor documentation regarding NCR’s ACS POS server and observed application files (see 3.2.x comments for application files reviewed) to determine that the following methods are used to render cardholder data unreadable within the POS environment:</p> <ul style="list-style-type: none"> <li>• 128-bit 3DES encryption</li> <li>• Truncation</li> </ul> <p>Additionally, Verizon Business reviewed RSA File Security Manager and RSA Key Manager applications, related to protecting sensitive data (including cardholder data) within Cisco’s PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable:</p> <ul style="list-style-type: none"> <li>• RSA File Security Manager – 192-bit 3DES or 256-bit AES encryption.</li> <li>• RSA Key Manager – 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES encryption.</li> </ul>		<p>Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider. At least one of the following methods must be used:</p> <ul style="list-style-type: none"> <li>• One-way hashes based on strong cryptography</li> <li>• Truncation</li> <li>• Index tokens and pads, with the pads being securely stored</li> <li>• Strong cryptography, with associated key-management processes and procedures</li> </ul>
--	--	--	--	--

	<b>3.4.b</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).	Verizon Business reviewed NCR's ACS POS server and POS register and confirmed that cardholder data was truncated or encrypted in all locations. Verizon Business also reviewed encryption capabilities for RSA File Security Manager and RSA Key Manager products. Verizon Business confirmed that all test files used during the review were successfully rendered unreadable using strong encryption.		<a href="#">See 3.4 above</a>
	<b>3.4.c</b> Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	N/A – Tape backups were not included in the scope of the review.		<a href="#">See 3.4 above</a>
	<b>3.4.d</b> Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.	Verizon Business reviewed NCR's ACS POS server and POS register and confirmed that cardholder data was truncated or encrypted in all locations. Verizon Business also reviewed encryption capabilities for RSA File Security Manager and RSA Key Manager products. Verizon Business confirmed that all test files used during the review were successfully rendered unreadable using strong encryption.		<a href="#">See 3.4 above</a>
<b>3.4.1</b> 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.	<b>3.4.1.a</b> 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).	N/A – Disk encryption was not used in the environment.		<a href="#">See 3.4 above</a>
	<b>3.4.1.b</b> Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	N/A – Disk encryption was not used in the environment.		<a href="#">Encryption / Key Management policies and procedures, including technical controls is the responsibility of the merchant / service provider.</a>
	<b>3.4.1.c</b> Verify that cardholder data on removable media is encrypted wherever stored. Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.	N/A – Disk encryption was not used in the environment.		<a href="#">See 3.4 above</a>

<p><b>3.5</b>Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:</p>	<p><b>3.5</b> Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:</p>			
<p><b>3.5.1</b> Restrict access to cryptographic keys to the fewest number of custodians necessary.</p>	<p><b>3.5.1</b>Examine user access lists to verify that access to keys is restricted to very few custodians.</p>	<p>Verizon Business confirmed that restricted access to encryption keys is as follows:</p> <ul style="list-style-type: none"> <li>• NCR ACS: Encryption keys are generated using the “Interactive Key Maintenance” tool. Only administrators have access to this tool. The encryption key is stored in an encrypted format within a binary file and is not disclosed to the key administrator at key generation time or at any other time.</li> <li>• RSA File Security Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys.</li> <li>• RSA Key Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA Key Manager security policies require public key authentication to access key material for encryption/decryption purposes.</li> </ul>		<p>Protection of encryption keys is the responsibility of the merchant / service provider.</p>

<p><b>3.5.2</b> Store cryptographic keys securely in the fewest possible locations and forms.</p>	<p><b>3.5.2</b> 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.</p>	<p>Verizon Business reviewed protection/storage for encryption keys and confirmed the following:</p> <ul style="list-style-type: none"> <li>• NCR ACS: Data encryption keys are stored in an encrypted format within the ENCKEY binary file. The key-encrypting key is statically compiled into the application.</li> <li>• RSA File Security Manager: The data encryption key is protected using a private RSA 1024-bit role key. The role key is encrypted using a unique access key. The access key is not stored on the system in its entirety, but is derived by seeding the PRNG with a SID (unique) and additional salt, resulting in unique key material for each user and process configured within FSM.</li> <li>• RSA Key Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database.</li> </ul>		<p>See 3.5.1 above</p>
<p><b>3.6</b> Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:</p>	<p><b>3.6.a</b> Verify the existence of key-management procedures for keys used for encryption of cardholder data.</p> <p> <b>Note</b> Numerous industry standards for key management are available from various resources including NIST, which can be found at <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>.</p>	<p>N/A – Key Management policy and procedures</p>		<p>Key Management policies and procedures is the responsibility of the merchant / service provider.</p>
	<p><b>3.6.b</b> For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider).</p>	<p>N/A – Key Management policy and procedures</p>		<p>See 3.6.a above</p>
	<p><b>3.6.c</b> Examine the key-management procedures and perform the following:</p>			

<p><b>3.6.1</b>Generation of strong cryptographic keys</p>	<p><b>3.6.1</b>Verify that key-management procedures are implemented to require the generation of strong keys.</p>	<p>Verizon Business confirmed that generation of strong keys is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> 128-bit 3DES keys</li> <li>• <b>RSA File Security Manager:</b> 192-bit 3DES or 256-bit AES keys</li> <li>• <b>RSA Key Manager:</b> 192-bit 3DES or 128-bit/192-bit/256-bit AES keys</li> </ul>		<p><a href="#">See 3.6.a above</a></p>
<p><b>3.6.2</b>Secure cryptographic key distribution</p>	<p><b>3.6.2</b>Verify that key-management procedures are implemented to require secure key distribution.</p>	<p>Verizon Business confirmed that secure distribution of keys is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> Encryption keys are generated locally, using the Interactive Key Maintenance tool and imported into the ENCKEY binary file.</li> <li>• <b>RSA File Security Manager:</b> Encryption keys are stored centrally on the RSA File Security Manager server and sent in encrypted format to the client system requiring encryption/decryption functions.</li> <li>• <b>RSA Key Manager:</b> All key transfers are done over SSLv3/TLSv1 connections between Key Manager server and Key Manager Clients.</li> </ul>		<p><a href="#">See 3.6.a above</a></p>
<p><b>3.6.3</b>Secure cryptographic key storage</p>	<p><b>3.6.3</b>Verify that key-management procedures are implemented to require secure key storage.</p>	<p>Verizon Business confirmed that secure key storage is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> Encryption keys are encrypted using a 128-bit 3DES key-encryption key.</li> <li>• <b>RSA File Security Manager:</b> The data encryption key is protected using a private RSA 1024-bit role key. The role key is encrypted using a unique access key (256-bit AES encryption). The access key is not persistently stored on the client system in its entirety, but is derived by seeding the PRNG with a SID (unique) and additional salt, resulting in unique key material for each user and process configured within FSM.</li> <li>• <b>RSA Key Manager:</b> Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database.</li> </ul>		<p><a href="#">See 3.6.a above</a></p>

<p><b>3.6.4</b>Periodic cryptographic key changes</p> <ul style="list-style-type: none"> <li>As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically</li> <li>At least annually</li> </ul>	<p><b>3.6.4</b>Verify that key-management procedures are implemented to require periodic key changes at least annually.</p>	<p>Verizon Business confirmed that key rotation capabilities are included for the following:</p> <ul style="list-style-type: none"> <li><b>NCR ACS:</b> New keys can be generated using the Interactive Key Maintenance tool. Data encrypted with a particular key is stored with a key index, so that multiple keys can be used for data encryption.</li> <li><b>RSA File Security Manager:</b> Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters decrypt “at rest” data and re-encrypt with new key.</li> <li><b>RSA Key Manager:</b> RSA Key Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Encryption keys can be assigned different key states, depending on known state of key. Examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised.</li> </ul>	<p>See 3.6.a above</p> <p><b>Note:</b> NCR ACS application. There was no reasonable way to rotate encryption keys, without manually decrypting all data and re-encrypting with a new key. NCR ACS application allows multiple keys (up to 255) to be used to limit the amount of data encrypted with a single key.</p>
<p><b>3.6.5</b>Retirement or replacement of old or suspected compromised cryptographic keys</p>	<p><b>3.6.5.a</b>Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).</p>	<p>Verizon Business confirmed that destruction of keys is included for the following:</p> <ul style="list-style-type: none"> <li><b>NCR ACS:</b> New keys can be generated using the Interactive Key Maintenance tool. Old keys can be removed from use or overwritten through the Interactive Key Maintenance tool.</li> <li><b>RSA File Security Manager:</b> Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters decrypt “at rest” data and re-encrypt with new key.</li> <li><b>RSA Key Manager:</b> RSA Key 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. States are assigned to encryption keys to limit transition use of key. Examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised.</li> </ul>	<p>See 3.6.a above</p>

	<p><b>3.6.5.b</b> Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.</p>	<p>Verizon Business confirmed that replacement of known or suspected compromised keys is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> Compromised keys can be removed or destroyed using the Interactive Key Maintenance tool.</li> <li>• <b>RSA File Security Manager:</b> Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters transparently decrypt “at rest” data and re-encrypt with new key.</li> <li>• <b>RSA Key Manager:</b> RSA Key Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Different states can be assigned to encryption keys in the event of a suspected or known key compromise. Key state examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised.</li> </ul>	<p><a href="#">See 3.6.a above</a></p>
--	--	---	--




<p><b>3.6.6</b> Split knowledge and establishment of dual control of cryptographic keys</p>	<p><b>3.6.6</b> Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).</p>	<p>Verizon Business confirmed that split knowledge/dual control of keys is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> Encryption keys are generated using the “Interactive Key Maintenance” tool. Only administrators have access to this tool. The encryption key is stored in an encrypted format within a binary file and is not disclosed to the key administrator at key generation time.</li> <li>• <b>RSA File Security Manager:</b> Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys. Additional roles exist within RSA File Security Manager to further segregate key management capabilities between “Security Admin” (responsible for management of security officers and has no visibility into encryption keys or security policies) and “Security Officers” (creates security policies, assigns encryption keys, but has no visibility into data being protected).</li> <li>• <b>RSA Key Manager:</b> Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format.</li> </ul>	<p><a href="#">See 3.6.a above</a></p>
---	--	--	--

<p><b>3.6.7</b>Prevention of unauthorized substitution of cryptographic keys</p>	<p><b>3.6.7</b>Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.</p>	<p>Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following:</p> <ul style="list-style-type: none"> <li>• <b>NCR ACS:</b> Encryption keys are generated using the “Interactive Key Maintenance” tool. Only administrators have access to this tool. CSA has also been installed on the ACS server and further restricts access, monitors access, and logs access to tools necessary for key replacement.</li> <li>• <b>RSA File Security Manager:</b> Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys. Additional roles exist within RSA File Security Manager to further segregate key management capabilities between “Security Admin” (responsible for management of security officers and has no visibility into encryption keys or security policies) and “Security Officers” (creates security policies, assigns encryption keys, but has no visibility into data being protected). Security Officers can only conduct key administration functions, they cannot access decrypted data, assuming separation of duties has been implemented on the client OS (e.g. key administrators are not users on the client system that uses encryption functions).</li> <li>• <b>RSA Key Manager:</b> 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.</li> </ul> <p>Additionally, Verizon Business confirmed that firewall segmentation and granular firewall access lists exist to further restrict access to POS systems and encryption key management servers.</p>	<p><a href="#">See 3.6.a above</a></p>
--	--	---	--

<b>3.6.8</b> Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	<b>3.6.8</b> Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.	N/A – Key custodian lists are the responsibility of the merchant/service provider.		<a href="#">See 3.6.a above</a>
---	--	--	--	---------------------------------

#### **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 can be continued 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	Target Date/ Comments
<p><b>4.1</b> Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p>Examples of open, public networks that are in scope of the PCI DSS are:</p> <ul style="list-style-type: none"> <li>• The Internet,</li> <li>• Wireless technologies,</li> <li>• Global System for Mobile communications (GSM), and</li> <li>• General Packet Radio Service (GPRS).</li> </ul>	<p><b>4.1.a</b> Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks</p> <ul style="list-style-type: none"> <li>• Verify that strong encryption is used during data transmission</li> <li>• For SSL implementations:                             <ul style="list-style-type: none"> <li>– Verify that the server supports the latest patched versions.</li> <li>– Verify that HTTPS appears as a part of the browser Universal Record Locator (URL).</li> <li>– Verify that no cardholder data is required when HTTPS does not appear in the URL.</li> </ul> </li> <li>• Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.</li> <li>• Verify that only trusted SSL/TLS keys/certificates are accepted.</li> <li>• Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)</li> </ul>	<p><b>4.1.a</b> Verizon Business reviewed the following configurations to confirm that secure transmission of cardholder data would be accomplished:</p> <ul style="list-style-type: none"> <li>• The wireless network within the large, medium, and small store environment (WPA (128-bit RC4 encryption))</li> <li>• 128-bit SSL (Secure FTP (SFTP) of cardholder data from store environment to PCI file server within data center). Cisco’s PCI solution would allow for both transmission of data over private circuit to the WAN edge of the data center, or over IPsec VPN back to data center.</li> <li>• Verizon Business confirmed that the proper encryption strength (128-bit RC4) has been implemented for all wireless traffic within the PCI Solution for Retail environment. Verizon business also confirmed the SFTP sever was configured with strong encryption.</li> </ul> <p> <b>Note</b> Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic.</p>		

<p><b>4.1.1</b> 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.</p> <ul style="list-style-type: none"> <li>For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</li> <li>For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</li> </ul>	<p><b>4.1.1</b> 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.</p>	<p>Verizon Business reviewed wireless settings within the PCI Solution for Retail environment to confirm WPA (128-bit RC4) encryption has been implemented for all wireless traffic.</p>		
<p><b>4.2</b> Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).</p>	<p><b>4.2.a</b> Verify that strong cryptography is used whenever cardholder data is sent via end-user messaging technologies.</p>	<p>N/A – Data Control / Encryption policy and procedures</p>		<p>Responsibility of merchant / service provider</p>
	<p><b>4.2.b</b> Verify the existence of a policy stating that unencrypted PANs are not to be sent via end-user messaging technologies.</p>	<p>N/A – Data Control / Encryption policy and procedures</p>		<p>Responsibility of merchant / service provider</p>

## 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 employees’ 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	Target Date/ Comments
<p>5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</p>	<p>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.</p>	<p>Verizon Business confirmed A/V software is installed on Windows systems within the PCI Solution for Retail environment; however, the assessment focus for PCI A/V requirements was placed on Cisco Security Agent software, and its ability to meet the intent of A/V requirements. Cisco Security Agent software is installed on the following Windows system components within the environment:</p> <ul style="list-style-type: none"> <li>• Cisco ACS console</li> <li>• WCS console</li> <li>• CiscoWorks (LMS, NCM) consoles</li> <li>• CSA console</li> <li>• CSM console</li> <li>• RSA Authentication Manager</li> <li>• RSA Access Manager</li> <li>• RSA File Security Manager</li> <li>• RSA Key Manager</li> <li>• NCR ACS Server</li> </ul> <p>Although Verizon Business recommends installing Anti-Virus software on the above system components, CSA software could be used, in conjunction with existing firewall segmentation and restricted Internet access, in order to mitigate the majority of common anti-virus risks (see comments).</p> <p><b>Important:</b> Because POS environments vary with each vendor, a full assessment of</p>		<p><b>Note:</b> CSA can be configured to protect against the following virus and malware threats:</p> <p>Virus propagation prevention through intrusion detection/prevention and port blocking</p> <p>Unauthorized/malicious application execution</p> <p>Application hijacking</p> <p>Buffer overflows</p> <p>Instant Messaging (IM can be configured through CSA policy to prohibit downloading files)</p> <p><b>Important:</b> Any attempt to use CSA as a compensating control for A/V would be subject to examination of the environment, the configuration of CSA</p>

		the POS environment, Internet/email connectivity to the POS environment, corporate connectivity to the POS environment, CSA configuration, and all compensating controls would need to be made for each merchant, in order to make an “In Place/Not in Place” assessment (If CSA software is used as a compensating control for Anti-Virus software).	and its ability to mitigate risks from virus threats, and the opinion of the individual assessor.
<b>5.1.1</b> Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	<b>5.1.1</b> 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).	See 5.1 above	See 5.1 above

<p>Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p><b>5.2</b> Verify that all anti-virus software is current, actively running, and capable of generating logs by performing the following:</p>	<p>Verizon Business observed A/V software installed on Windows components within the PCI Solution for Retail environment. Verizon Business also reviewed vendor documentation and observed a demo of CSA's capabilities to provide layered security through multiple security controls. The PCI Solution for Retail environment implementation addresses the following AV requirements (5.2.b and 3<sup>rd</sup> bullet items):</p>	<p><b>Important:</b> Any attempt to use CSA as a compensating control for A/V would be subject to examination of the environment, the configuration of CSA and its ability to mitigate risks from virus threats, and the opinion of the individual assessor.</p>
	<p><b>5.2.a</b> Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.</p>	<p>N/A – Written A/V policy</p>	<p>Responsibility of merchant / service provider</p>
	<p><b>5.2.b</b> Verify that the master installation of the software is enabled for automatic updates and periodic scans.</p>	<p>Verizon Business confirmed a central (master) console for CSA exists in the PCI Solution for Retail environment, which centrally manages all CSA client policies.</p>	
	<p><b>5.2.c</b> 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.</p>	<p>Verizon Business confirmed a central (master) console for CSA exists in the PCI Solution for Retail environment, which centrally manages all CSA client policies. As</p>	
	<p><b>5.2.d</b> 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</p>	<p>N/A – Central storage and retention of A/V logs is the responsibility of the merchant / service provider</p>	<p>PCI DSS v1.2 now requires that anti-virus logs be retained in accordance with PCI DSS requirement 10.7.b (minimum of 90 days online and 1 year online/on tape).</p>

**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	Target Date/ Comments
<p><b>6.1</b>Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.</p> <p><i>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.</i></p>	<p><b>6.1.a</b>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.</p>	Verizon Business reviewed configurations for the PCI Solution for Retail environment 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 (Feb 2008).		
	<p><b>6.1.b</b>Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.</p>	N/A – Patch management policy and procedures		Patch management policies and procedures is the responsibility of the merchant / service provider.

### 3. Details about Reviewed Environment

<p><b>6.2</b> Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.</p>	<p><b>6.2.a</b> Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.</p>	<p>N/A – Patch / Risk management policy and procedures</p>	<p>Patch / Risk management procedures are the responsibility of the merchant / service provider.</p>
	<p><b>6.2.b</b> Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.</p>	<p>Verizon Business reviewed vendor documentation for CiscoWorks (LMS) and confirmed its ability to generate upgrade reports for active devices under CiscoWorks configuration management.</p>	<p>Overall Patch / Risk management procedures are 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.</p>
<p><b>6.3</b> Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:</p>	<p><b>6.3.a</b> Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS.</p>	<p>N/A – SDLC policy/procedures</p>	<p>SDLC processes are the responsibility of the merchant / service provider.</p>
	<p><b>6.3.b</b> From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:</p>	<p>N/A – SDLC policy/procedures</p>	<p>SDLC processes are the responsibility of the merchant / service provider.</p>
<p><b>6.3.1</b> Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:</p>	<p><b>6.3.1</b> All changes (including patches) are tested before being deployed into production.</p>	<p>N/A – SDLC policy/procedures</p>	<p>SDLC processes are the responsibility of the merchant / service provider.</p>
<p><b>6.3.1.1</b> Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)</p>	<p><b>6.3.1.1</b> Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)</p>	<p>N/A – SDLC policy/procedures</p>	<p>SDLC processes are the responsibility of the merchant / service provider.</p>
<p><b>6.3.1.2</b> Validation of proper error handling</p>	<p><b>6.3.1.2</b> Validation of proper error handling</p>	<p>N/A – SDLC policy/procedures</p>	<p>SDLC processes are the responsibility of the merchant / service provider.</p>

<b>6.3.1.3</b> Validation of secure cryptographic storage	<b>6.3.1.3</b> Validation of secure cryptographic storage	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.1.4</b> Validation of secure communications	<b>6.3.1.4</b> Validation of secure communications	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.1.5</b> Validation of proper role-based access control (RBAC)	<b>6.3.1.5</b> Validation of proper role-based access control (RBAC)	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.2</b> Separate development/test and production environments	<b>6.3.2</b> The development/test environments are separate from the production environment, with access control in place to enforce the separation.	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.3</b> Separation of duties between development/test and production environments	<b>6.3.3</b> There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.4</b> Production data (live PANs) are not used for testing or development	<b>6.3.4</b> Production data (live PANs) are not used for testing and development, or are sanitized before use.	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.5</b> Removal of test data and accounts before production systems become active	<b>6.3.5</b> Test data and accounts are removed before a production system becomes active.	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<b>6.3.6</b> Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	<b>6.3.6</b> Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.

### 3. Details about Reviewed Environment

<p><b>6.3.7</b> Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability</p> <p><i>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. 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.</i></p>	<p><b>6.3.7.a</b> Obtain and review policies to confirm all custom application code changes for <i>internal applications</i> must be reviewed (either using manual or automated processes), as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Appropriate corrections are implemented prior to release.</li> <li>• Code review results are reviewed and approved by management prior to release.</li> </ul>	<p>N/A – SDLC policy/procedures</p>		<p>SDLC processes are the responsibility of the merchant / service provider.</p>
	<p><b>6.3.7.b</b> Obtain and review policies to confirm that all custom application code changes for <i>web applications</i> must be reviewed (using either manual or automated processes) as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Code reviews ensure code is developed according to secure coding guidelines such as the <i>Open Web Security Project Guide</i> (see PCI DSS Requirement 6.5).</li> <li>• Appropriate corrections are implemented prior to release.</li> <li>• Code review results are reviewed and approved by management prior to release.</li> </ul>	<p>N/A – SDLC policy/procedures</p>		<p>SDLC processes are the responsibility of the merchant / service provider.</p>
	<p><b>6.3.7.c</b> Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.7a and 6.3.7b above.</p>	<p>N/A – SDLC policy/procedures</p>		<p>SDLC processes are the responsibility of the merchant / service provider.</p>

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.4 Follow change control procedures for all changes to system components. The procedures must include the following:	6.4.a Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below.			
	6.4.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.1 Documentation of impact	6.4.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change.	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.2 Management sign-off by appropriate parties	6.4.2 Verify that management sign-off by appropriate parties is present for each sampled change.	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.3 Testing of operational functionality	6.4.3 Verify that operational functionality testing is performed for each sampled change.	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.4 Back-out procedures	6.4.4 Verify that back-out procedures are prepared for each sampled change	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.

<p><b>6.5</b>Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the <i>Open Web Application Security Project Guide</i>. Cover prevention of common coding vulnerabilities in software development processes, to include the following:</p> <p>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</p>	<p><b>6.5.a</b>Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the OWASP guide (<a href="http://www.owasp.org">http://www.owasp.org</a>).</p>	<p>N/A – Web-based application development (secure coding) not in scope for assessment</p>	<p>Web-based software development processes, including secure coding practices, are the responsibility of the merchant / service provider. In scope web-based applications include external and internal applications which process or transmit cardholder data.</p> <p>Cisco installed Foundstrone’s “Hacme Bank” application. Hacme Bank simulates a "real-world" online banking application, which is built with a number of known and common vulnerabilities such as SQL injection and cross-site scripting. This allows users to attempt real exploits against a web application, and thus learn the specifics of the issue and how best to fix it. In addition, external websites were used to demonstrate Cisco XML Gateway’s capabilities. Verizon Business observed the use of Cisco’s ACE XML Gateway to protect against common web vulnerabilities and web based attacks identified under 6.5.1 – 6.5.10 (See 6.5.1 – 6.5.10 for specific details).</p>
	<p><b>6.5.b</b> Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.</p>		
	<p><b>6.5.c</b>Verify that processes are in place to ensure that web applications are not vulnerable to the following:</p>		

<p><b>6.5.1</b>Cross-site scripting (XSS)</p>	<p><b>6.5.1</b>Cross-site scripting (XSS) (Validate all parameters before inclusion.)</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based XSS attacks. For example, ACE XML Gateway can prevent submission of XML and HTML tags to the web server (required for XSS attacks). All XSS attacks were manual and required custom configuration of the ACE XML Gateway application.</p>	<p><a href="#">See 6.5.a above</a></p>
<p><b>6.5.2</b>Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.</p>	<p><b>6.5.2</b>Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based injection attacks, including SQL injection. Limiting input to specific criteria, including restricting required characters/strings for SQL attacks, was demonstrated to prevent such attacks. All SQL injection attacks were manual and required custom configuration of the ACE XML Gateway application.</p>	<p><a href="#">See 6.5.a above</a></p>
<p><b>6.5.3</b>Malicious file execution</p>	<p><b>6.5.3</b>Malicious file execution (Validate input to verify application does not accept filenames or files from users.)</p>		<p>This vulnerability is new to the OWASP guide since the last assessment of the ACE XML Gateway. As such, the ACE XML Gateway was not assessed at that time to determine capabilities to prevent malicious file execution. This prevention capability will be assessed within the next six months as part of the next PCI Solution for Retail phase.</p>

<p><b>6.5.4</b>Insecure direct object references</p>	<p><b>6.5.4</b>Insecure direct object references (Do not expose internal object references to users.)</p>		<p>This vulnerability is new to the OWASP guide since the last assessment of the ACE XML Gateway. As such, the ACE XML Gateway was not assessed at that time to determine capabilities to prevent insecure direct object references. This prevention capability will be assessed within the next six months as part of the next PCI Solution for Retail phase.</p>
<p><b>6.5.5</b>Cross-site request forgery (CSRF)</p>	<p><b>6.5.5</b>Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)</p>		<p>This vulnerability is new to the OWASP guide since the last assessment of the ACE XML Gateway. As such, the ACE XML Gateway was not assessed at that time to determine capabilities to prevent cross-site request forgery (CSRF). This prevention capability will be assessed within the next six months as part of the next PCI Solution for Retail phase.</p>
<p><b>6.5.6</b>Information leakage and improper error handling</p>	<p><b>6.5.6</b>Information leakage and improper error handling (Do not leak information via error messages or other means.)</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based information leakage and improper error handling vulnerabilities. HTML/XML errors from the web server can be intercepted by the ACE XML Gateway and re-written as a generic, non-descript error message. This was demonstrated during the review. All error handling attacks were manual and required custom configuration of the ACE XML Gateway application to prevent improper error handling.</p>	<p>See 6.5.a above</p>



<p><b>6.5.7</b>Broken authentication and session management</p>	<p><b>6.5.7</b>Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)</p>		<p>See 6.5.a above</p> <p>Examples of broken authentication and session management prevention were not demonstrated. Such prevention could be demonstrated through secure web-coding and clean results from vulnerability scanning/penetration testing for such vulnerabilities. Additionally, Cisco is working to address additional XML and HTML based web-vulnerabilities in future releases of the product.</p>
<p><b>6.5.8</b>Insecure cryptographic storage</p>	<p><b>6.5.8</b>Insecure cryptographic storage (Prevent cryptographic flaws.)</p>		<p>See 6.5.a above</p> <p>Insecure cryptographic storage is not designed to be prevented by the ACE XML Gateway. Secure storage should be addressed through secure coding and secure web application architecture, which includes implementation of best-practice encryption/key management for storage of sensitive data.</p>
<p><b>6.5.9</b>Insecure communications</p>	<p><b>6.5.9</b>Insecure communications (Properly encrypt all authenticated and sensitive communications.)</p>		

<p><b>6.5.10</b> Failure to restrict URL access</p>	<p><b>6.5.10</b> Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)</p>		
<p><b>6.6</b> For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by <i>either</i> of the following methods:</p> <ul style="list-style-type: none"> <li>Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes</li> <li>Installing a web-application firewall in front of public-facing web applications</li> </ul>	<p><b>6.6</b> For <i>public-facing</i> web applications, ensure that <i>either</i> one of the following methods are in place as follows:</p> <ul style="list-style-type: none"> <li>Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: <ul style="list-style-type: none"> <li>At least annually</li> <li>After any changes</li> <li>By an organization that specializes in application security</li> <li>That all vulnerabilities are corrected</li> <li>That the application is re-evaluated after the corrections</li> </ul> </li> <li>Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks.</li> </ul> <p><b>Note:</b> “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.</p>		<p>Since the last assessment of the ACE XML Gateway (December 2007), the OWASP Guideline has introduced a number of new web-application attack vectors and vulnerabilities which should be prevented by an acceptable web-application firewall solution. Since the ACE XML Gateway has not been assessed against the new Top 10 OWASP vulnerabilities, the assessor cannot make a determination as to its ability to meet this requirement at this time. The ACE XML Gateway will be assessed against the new OWASP Top 10 within the next 6 months, as part of the next PCI Solution for Retail phase.</p>

## 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	Target Date/ 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:	N/A – Security Policy (Data Control / Data Classification)		Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.
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.	N/A – Security Policy (Data Control / Data Classification)		Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.
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).	N/A – Security Policy (Data Control / Data Classification)		Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.

<p><b>7.1.3</b> Requirement for an authorization form signed by management that specifies required privileges</p>	<p><b>7.1.3</b> Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.</p>	<p>N/A – Security Policy (Data Control / Data Classification)</p>		<p>Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.</p>
<p><b>7.1.4</b> Implementation of an automated access control system</p>	<p><b>7.1.4</b> Confirm that access controls are implemented via an automated access control system.</p>	<p>N/A – Security Policy (Data Control / Data Classification)</p>		<p>Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.</p>
<p><b>7.2</b> 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:</p>	<p><b>7.2</b> Examine system settings and vendor documentation to verify that an access control system is implemented as follows:</p>	<p>Verizon Business reviewed system settings, EMC SAN storage (zoning and LUN masking configuration), vendor documentation, and interviewed SMEs for platforms within the PCI Solution for Retail environment to confirm access control systems within the environment include the following:</p>		

<p><b>7.2.1</b>Coverage of all system components</p>	<p>Confirm that access control systems are in place on all system components.</p>	<p>Verizon Business confirmed that access control systems are in place on the following reviewed system components:</p> <p>Coverage of all system components within the PCI Solution for Retail environment:</p> <ul style="list-style-type: none"> <li>• WCS (wireless console)</li> <li>• Cisco ACS (authentication for all network components (e.g. ISRs, routers, switches, and wireless controllers)</li> <li>• CiscoWorks (LMS, NCM)</li> <li>• CSM (Cisco Security Manager)</li> <li>• CSA Manager</li> <li>• CS-MARS</li> <li>• ACE XML Gateway (direct SSH or https – auth forwards to ACS -&gt; AD)</li> <li>• ASA and FWSM firewalls (direct SSH or ASDM – forwards to ACS -&gt; AD)</li> <li>• ISRs (direct SSH or SDM – auth forwards to ACS -&gt; AD)</li> <li>• Routers and switches (direct ssh access forwards authentication to ACS -&gt; AD)</li> <li>• Wireless controllers (direct ssh access forwards authentication to ACS -&gt; AD)</li> <li>• Cisco IDSM-2 modules (direct SSH or IDM – local auth)</li> <li>• RSA Authentication Manager</li> <li>• RSA Access Manager</li> <li>• RSA File Security Manager</li> <li>• RSA Key Manager</li> <li>• RSA enVision</li> <li>• NCR ACS Server</li> <li>• CSA client software provides additional access control protection at the OS level for POS systems and all management consoles running on Windows. CSA can be configured to restrict, monitor, and alert on access to OS/application binaries, configuration and log files</li> </ul>		
--	---	--	--	--

<p><b>7.2.2</b>Assignment of privileges to individuals based on job classification and function</p>	<p>Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.</p>	<p>Verizon Business confirmed that access control systems include role-based privilege assignment for all management consoles (e.g. WCS, ACS, CSA, CiscoWorks (LMS, NCM), CSM, CS-MARS, ACE XML Gateway, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, RSA enVision, and NCR ACS Server)</p>		
<p><b>7.2.3</b>Default “deny-all” setting</p>	<p>Confirm that the access control systems has a 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.</p>	<p>Verizon Business confirmed that access control systems include default “deny-all” settings on all management consoles and network devices. ASA firewalls, FWSMs, and ISRs contain “default-deny” access lists with explicit “permit” rules defined to the port level.</p>		

**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.



PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
----------------------	--------------------	----------	--------------	--------------------------



<p><b>8.1</b>Assign all users a unique ID before allowing them to access system components or cardholder data.</p>	<p><b>8.1</b>Verify that all users are assigned a unique ID for access to system components or cardholder data.</p>	<p>Verizon Business reviewed access lists for the following, to confirm all users have a unique username for access to components within the PCI Solution for Retail environment:</p> <ul style="list-style-type: none"> <li>• CS-MARS</li> <li>• WCS central wireless server</li> <li>• Cisco ACS</li> <li>• Cisco Security Agent (CSA) Manager</li> <li>• CSM (Cisco Security Manager)</li> <li>• CiscoWorks (LMS)</li> <li>• Cisco ASDM</li> <li>• All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts.</li> <li>• Cisco ACE XML Gateway</li> <li>• CiscoWorks NCM</li> <li>• Cisco IDM</li> <li>• RSA enVision</li> <li>• RSA Key Manager</li> <li>• RSA Access Manager</li> <li>• RSA Authentication Manager (unique PIN + tokencode)</li> <li>• RSA File Security Manager – RSA File Security Manager does not support renaming the default Security Admin “SA” account. Only one SA account is allowed, so this generic account must be used for all SA functions within RSA File Security Manager. In the Cisco lab environment the RSA File Security Manager system is accessed over RDP. This would allow unique AD credentials to be captured for system access. Additionally, Cisco leveraged CSA software to further restrict, monitor, and log access to the RSA File Security Manager executable.</li> <li>• NCR ACS Server (unique AD credentials)</li> </ul>		
--	---	---	--	--

<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>▪ Password or passphrase</li> <li>▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>• Obtain and examine documentation describing the authentication method(s) used.</li> <li>• 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).</li> </ul>	<p>Verizon Business reviewed authentication methods, including observation of live login attempts to confirm a unique ID and password was required for each authentication attempt to the following:</p> <ul style="list-style-type: none"> <li>• CS-MARS</li> <li>• WCS central wireless server</li> <li>• Cisco ACS</li> <li>• Cisco Security Agent (CSA) Manager</li> <li>• CSM (Cisco Security Manager)</li> <li>• CiscoWorks (LMS)</li> <li>• Cisco ASDM</li> <li>• All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts.</li> <li>• Cisco ACE XML Gateway</li> <li>• CiscoWorks NCM</li> <li>• Cisco IDM</li> <li>• RSA enVision</li> <li>• RSA Key Manager</li> <li>• RSA Access Manager</li> <li>• RSA Authentication Manager (unique PIN + tokencode)</li> <li>• RSA File Security Manager (see 8.1 above)</li> <li>• NCR ACS Server (AD auth)</li> </ul>		
--	---	---	--	--

<p><b>8.3</b> Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</p>	<p><b>8.3</b>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 both a password and an additional authentication item (for example, smart card, token, PIN) are required.</p>	<p>Verizon Business confirmed the use of two-factor authentication, using RSA SecurID PINs + tokencode for all remote authentication into the data center environment.</p>	<p>Two-factor authentication for all remote access, including for employees, contractors, and third parties, is the responsibility of the merchant / service provider.</p>
--	--	--	--

<p><b>8.4</b>Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in <i>PCI DSS Glossary of Terms, Abbreviations, and Acronyms</i>).</p>	<p><b>8.4.a</b>For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.</p>	<p>Verizon Business confirmed local ISR and switch passwords are rendered unreadable, per review of configurations. All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which renders passwords unreadable. Authentication to CSA Manager is forwarded directly to Active Directory.</p> <p>Verizon Business also confirmed the following render local authentication credentials unreadable:</p> <ul style="list-style-type: none"> <li>• WCS (hashed)</li> <li>• CS-MARS (hashed)</li> <li>• Cisco ACE XML Gateway (hashed)</li> <li>• Cisco IDM (hashed)</li> <li>• CiscoWorks NCM (hashed)</li> <li>• RSA enVision (encrypted hash)</li> <li>• RSA Key Manager (Auth through RSA Access Manager (hashed), local auth (hashed))</li> <li>• RSA Access Manager (hashed)</li> <li>• RSA File Security Manager (hashed)</li> <li>• NCR ACS (AD auth – passwords unreadable)</li> </ul>		<ul style="list-style-type: none"> <li>• RSA Authentication Manager (Evidence for RSA Authentication Manager was not provided)</li> </ul>
	<p><b>8.4.b</b>For service providers only, observe password files to verify that customer passwords are encrypted.</p>	<p>N/A – Service Provider requirement</p>		<p>Responsibility of service provider.</p>

<p><b>8.5</b>Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:</p>	<p><b>8.5</b>Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:</p>		
<p><b>8.5.1</b>Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.</p>	<p><b>8.5.1.a</b>Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following:</p> <ul style="list-style-type: none"> <li>• Obtain and examine an authorization form for each ID.</li> <li>• 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.</li> </ul>	<p>N/A – Security policy and procedures (ID / Account Management)</p>	<p>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.</p>
<p><b>8.5.2</b>Verify user identity before performing password resets.</p>	<p><b>8.5.2</b>Examine password 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.</p>	<p>N/A – Security policy and procedures (ID / Account Management)</p>	<p>Account management / password reset procedures are the responsibility of the merchant / service provider.</p>

<p><b>8.5.3</b>Set first-time passwords to a unique value for each user and change immediately after the first use.</p>	<p><b>8.5.3</b>Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use.</p>	<p>N/A – Security policy and procedures (ID / Account Management)</p>	<p>Account management / password reset procedures are the responsibility of the merchant / service provider.</p>
<p><b>8.5.4</b>Immediately revoke access for any terminated users.</p>	<p><b>8.5.4</b>Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.</p>	<p>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.</p>	
<p><b>8.5.5</b>Remove/disable inactive user accounts at least every 90 days.</p>	<p><b>8.5.5</b>Verify that inactive accounts over 90 days old are either removed or disabled.</p>	<p>N/A – Manual audit procedure or third party ID management tool.</p>	<p><b>Note:</b> Because most authentication systems, including Active Directory, do not have built-in audit tools to easily identify inactive user accounts, manual procedures or third party tools are necessary to identify and remove inactive accounts.</p>
<p><b>8.5.6</b>Enable accounts used by vendors for remote maintenance only during the time period needed.</p>	<p><b>8.5.6</b>Verify that any accounts used by vendors to support and maintain system components are disabled, enabled only when needed by the vendor, and monitored while being used.</p>	<p>N/A – No external vendor accounts were identified during the assessment.</p>	
<p><b>8.5.7</b>Communicate password procedures and policies to all users who have access to cardholder data.</p>	<p><b>8.5.7</b>Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies.</p>	<p>N/A – Security Policy (Security Awareness)</p>	<p>For each merchant / service provider - Individual interviews to be conducted with a sample of users to confirm security awareness for password procedures is in place.</p>

<p><b>8.5.8</b> Do not use group, shared, or generic accounts and passwords.</p>	<p><b>8.5.8.a</b> For a sample of system components, examine user ID lists to verify the following</p> <ul style="list-style-type: none"> <li>• Generic user IDs and accounts are disabled or removed.</li> <li>• Shared user IDs for system administration activities and other critical functions do not exist.</li> <li>• Shared and generic user IDs are not used to administer any system components.</li> </ul>	<p>Verizon Business reviewed user ID lists for the following components within the PCI Solution for Retail environment to confirm generic and shared IDs are disabled or removed, or that unique administrative accounts are used in place of default accounts that cannot be renamed or removed:</p> <ul style="list-style-type: none"> <li>• CS-MARS</li> <li>• WCS central wireless server</li> <li>• Cisco ACS</li> <li>• Cisco Security Agent (CSA) Manager</li> <li>• CSM (Cisco Security Manager)</li> <li>• CiscoWorks (LMS)</li> <li>• Cisco ASDM</li> <li>• All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts.</li> <li>• Cisco ACE XML Gateway</li> <li>• CiscoWorks NCM</li> <li>• Cisco IDM</li> <li>• RSA enVision</li> <li>• RSA Key Manager</li> <li>• RSA Access Manager</li> <li>• RSA Authentication Manager</li> <li>• NCR ACS</li> </ul>		<p><b>Note:</b> “pnadmin” account on CS-MARS cannot be deleted, due to application dependencies. This account is not used interactively. All administrative accounts are unique. Additionally, RSA File Security Manager “SA” account cannot be deleted, and is the only Security Admin account on the system. See 8.1 for compensating controls used to restrict RSA File Security Manager access and capture unique credentials for RSA File Security Manager access.</p>
	<p><b>8.5.8.b</b> Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.</p>	<p>N/A – Security Policy (Password policy/procedures)</p>		<p>Password policy/procedures are the responsibility of each merchant / service provider.</p>
	<p><b>8.5.8.c</b> Interview system administrators to verify that group and shared passwords are not distributed, even if requested.</p>	<p>N/A – Security Policy (Password policy/procedures)</p>		<p>Password policy/procedures are the responsibility of each merchant / service provider.</p>

<p><b>8.5.9</b>Change user passwords at least every 90 days.</p>	<p><b>8.5.9</b>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.</p> <p>For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which is set to expire passwords after 42 days.</li> <li>• CSA Manager (AD auth = 42 days)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = 42 days)</li> <li>• Cisco ACS (Local ACS auth – 30 day expiration)</li> <li>• CS-MARS (AD auth through Cisco ACS = 42 days)</li> <li>• WCS (AD auth through Cisco ACS = 42 days)</li> <li>• CiscoWorks NCM (ACS or AD auth)</li> <li>• RSA enVision (ACS or AD auth = 42 days)</li> <li>• RSA Key Manager (RSA Access Manager auth = 60 days)</li> <li>• RSA Access Manager (60 days)</li> <li>• RSA Authentication Manager (tokencode changes every 60 seconds)</li> <li>• NCR ACS (AD auth = 42 days)</li> </ul>	<p>The following do not currently support password expiration, and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>- Cisco IDM</li> <li>- RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> A combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>
--	---	---	---	--



<p><b>8.5.10</b>Require a minimum password length of at least seven characters.</p>	<p><b>8.5.10</b>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.</p> <p>For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces passwords to contain a minimum of 7 characters.</li> <li>• CSA Manager (AD Auth = min 7 chars)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = min 7 chars, local auth= 8 characters)</li> <li>• CS-MARS (AD auth through Cisco ACS = min 7 chars)</li> <li>• Cisco ACS (local ACS auth = 8 character minimum)</li> <li>• WCS (AD auth through Cisco ACS = min 7 chars)</li> <li>• CiscoWorks NCM (ACS or AD auth, local auth= 8 characters)</li> <li>• RSA enVision (ACS or AD auth = min 7 chars)</li> <li>• RSA Key Manager (RSA Access Manager auth = 8 characters)</li> <li>• RSA Access Manager (8 characters)</li> <li>• RSA Authentication Manager (PIN + tokencode = min 10, max 16)</li> <li>• NCR ACS (AD auth = min 7 chars)</li> </ul>	<p>The following do not currently enforce password complexity (e.g. length, alpha-numeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>• Cisco IDM</li> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> A combination of documented password policies, manual audit procedures to ensure strong password generation, using periodic dictionary attacks against passwords, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>
---	--	--	--	--

<p><b>8.5.11</b> Use passwords containing both numeric and alphabetic characters.</p>	<p><b>8.5.11</b> 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. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), and CSM) are forwarded to Active Directory, which enforces alpha-numeric passwords.</li> <li>• CSA Manager (AD Auth = alpha-numeric)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = alpha-numeric)</li> <li>• Cisco ACS (local ACS auth = alpha-numeric)</li> <li>• CS-MARS (AD auth through Cisco ACS = alpha-numeric)</li> <li>• WCS (AD auth through Cisco ACS = alpha-numeric)</li> <li>• CiscoWorks NCM (ACS or AD auth = alpha-numeric, local auth requires upper/lower case + at least 1 special character or digit)</li> <li>• RSA enVision (ACS or AD auth = alpha-numeric)</li> <li>• RSA Key Manager (RSA Access Manager auth = alpha-numeric + dictionary check)</li> <li>• RSA Access Manager (alpha-numeric + dictionary check)</li> <li>• RSA Authentication Manager (supports alpha-numeric)</li> <li>• NCR ACS (AD auth = alpha-numeric)</li> </ul>	<p>The following do not currently enforce password complexity (e.g. length, alpha-numeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>• Cisco IDM</li> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> A combination of documented password policies, manual audit procedures to ensure strong password generation, using periodic dictionary attacks against passwords, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>
---	---	---	--	--

<p><b>8.5.12</b> 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.</p>	<p><b>8.5.12</b> 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.</p> <p>For service providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces password history for the last 24 passwords.</li> <li>• - CSA Manager (AD Auth = last 24 passwords)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = last 24 passwords)</li> <li>• Cisco ACS (local ACS auth = last 5 passwords)</li> <li>• CS-MARS (AD auth through Cisco ACS = last 24 passwords)</li> <li>• WCS (AD auth through Cisco ACS = last 24 passwords)</li> <li>• CiscoWorks NCM (ACS or AD auth = last 24 passwords)</li> <li>• RSA enVision (ACS or AD auth = last 24 passwords)</li> <li>• RSA Key Manager (RSA Access Manager auth = last 10 passwords)</li> <li>• RSA Access Manager (last 10 passwords)</li> <li>• RSA Authentication Manager (tokencode changes to random value every 60 seconds)</li> <li>• NCR ACS (AD auth = last 24 passwords)</li> </ul>	<p>The following do not currently enforce password complexity (e.g. length, alpha-numeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>• Cisco IDM (will be addressed in Cisco IDM v6.1 release)</li> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> A combination of documented password policies and internal firewall segmentation of these components within the data center would be reasonable compensating controls for password setting limitations within these applications.</p>
---	---	---	--	---

<p><b>8.5.13</b>Limit repeated access attempts by locking out the user ID after not more than six attempts.</p>	<p><b>8.5.13</b>For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a user’s account is locked out after not more than six invalid logon attempts.</p> <p>For service providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces account lockouts after 5 invalid logon attempts.</li> <li>• CSA Manager (AD Auth = 5 invalid attempts)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = 5 invalid attempts, local auth= 3 invalid attempts)</li> <li>• Cisco ACS (local ACS auth = 6 invalid attempts)</li> <li>• CS-MARS (AD auth through Cisco ACS = 5 invalid attempts)</li> <li>• WCS (AD auth through Cisco ACS = 5 invalid attempts)</li> <li>• CiscoWorks NCM (ACS or AD auth = 5 invalid attempts, local auth= 6 invalid attempts)</li> <li>• Cisco IDM (5 invalid attempts)</li> <li>• RSA enVision (ACS or AD auth = 5 invalid attempts)</li> <li>• RSA Key Manager (RSA Access Manager auth = 3 invalid attempts in one day)</li> <li>• RSA Access Manager (3 invalid attempts in one day)</li> <li>• RSA Authentication Manager (3 invalid passcodes forces “next token” mode, which requires two consecutive token codes to be entered. 6 failed attempts disables token use)</li> <li>• NCR ACS (AD auth = 5 invalid attempts)</li> </ul>	<p>The following do not currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> Using CSA or other monitoring software to alert on continuous invalid logon attempts, combined with internal firewall segmentation of these components, would be reasonable compensating controls for account lockout setting limitations within these applications.</p>
---	---	---	---	--

<p><b>8.5.14</b>Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.</p>	<p><b>8.5.14</b>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.</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> <li>• All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces account lockouts for 30 minutes.</li> <li>• CSA Manager (AD Auth = 30 min lockout)</li> <li>• Cisco ACE XML Gateway (ACS or AD auth = 30 min lockout, local auth= admin must reset)</li> <li>• Cisco ACS (local ACS auth = admin must reset)</li> <li>• CS-MARS (AD auth through Cisco ACS = 30 min lockout)</li> <li>• WCS (AD auth through Cisco ACS = 30 min lockout)</li> <li>• CiscoWorks NCM (ACS or AD auth = 30 min lockout, local auth= admin must reset)</li> <li>• Cisco IDM (Admin must reset)</li> <li>• RSA enVision (ACS or AD auth = 30 min lockout)</li> <li>• RSA Key Manager (RSA Access Manager auth = admin must reset)</li> <li>• RSA Access Manager (admin must reset)</li> <li>• RSA Authentication Manager (admin must reset)</li> <li>• NCR ACS (AD auth = 30 min lockout)</li> </ul>	<p>The following do not currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> Using CSA or other monitoring software to alert on continuous invalid logon attempts, combined with internal firewall segmentation of these components, would be reasonable compensating controls for account lockout setting limitations within these applications.</p>
---	---	---	---	--

<p><b>8.5.15</b>If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.</p>	<p><b>8.5.15</b>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.</p>	<p>Verizon Business confirmed the following components within the PCI Solution for Retail environment have sufficient idle timeout settings:</p> <ul style="list-style-type: none"> <li>• ISRs and switches: (15 minute session-timeout and 15 minute exec-timeout)</li> <li>• ASA firewalls (15 minutes – ssh)</li> <li>• Wireless controllers (15 minutes – ssh)</li> <li>• CiscoWorks (LMS): (15 minutes)</li> <li>• CS-MARS: (15 minutes)</li> <li>• CSM Manager: (15 minutes)</li> <li>• Cisco ACS: (15 minutes)</li> <li>• CSA Manager: (15 minutes)</li> <li>• Cisco ACE XML Gateway (15 minutes)</li> <li>• CiscoWorks NCM (15 minutes)</li> <li>• RSA enVision (10 minutes)</li> <li>• RSA Key Manager (15 minutes)</li> <li>• RSA Access Manager (10 minutes)</li> <li>• NCR ACS (configurable to 1 minute)</li> </ul>	<p>The following do not support idle session timeouts (15 minutes or less) for administrative connections:</p> <ul style="list-style-type: none"> <li>• WCS</li> <li>• IDM</li> <li>• Wireless controllers (web interface)</li> <li>• ASDM</li> <li>• IDM</li> <li>• RSA File Security Manager (to be addressed in FSM v2.2 release)</li> <li>• RSA Authentication Manager</li> </ul>	<p><b>Note:</b> Screensaver timeouts can be used as a compensating control, when idle session timeouts are not available or impact application/business operations (e.g. backup jobs).</p>
---	---	--	---	--

<p><b>8.5.16</b>Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.</p>	<p><b>8.5.16.a</b>Review database and application configuration settings and verify that user authentication and access to databases includes the following:</p> <ul style="list-style-type: none"> <li>• All users are authenticated prior to access.</li> <li>• 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).</li> <li>• Direct access or queries to databases are restricted to database administrators.</li> </ul>	<p>N/A – Database security not part of the PCI Solution for Retail environment assessment.</p>		<p><b>Note:</b> Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.</p>
	<p><b>8.5.16.b</b>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).</p>	<p>N/A – Database security not part of the PCI Solution for Retail environment assessment.</p>		<p><b>Note:</b> Database security, including prohibiting direct SQL queries to the database is the responsibility of the merchant / service provider. Database login accounts should be limited to application accounts and very few dba accounts.</p>

### 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.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
<p><b>9.1</b> Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.</p>	<p><b>9.1</b> Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.</p> <ul style="list-style-type: none"> <li>Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.</li> <li>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.</li> </ul>	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<p><b>9.1.1</b> Use video cameras or other 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.</p> <p>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.</p>	<p><b>9.1.1</b> Verify that video cameras or other access control mechanisms are in place to monitor the entry/exit points to sensitive areas. Video cameras or other mechanisms should be protected from tampering or disabling. Verify that video cameras or other mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.</p>	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<p><b>9.1.2</b> Restrict physical access to publicly accessible network jacks.</p>	<p><b>9.1.2</b> Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.</p>	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.



<p><b>9.1.3</b> Restrict physical access to wireless access points, gateways, and handheld devices.</p>	<p><b>9.1.3</b> Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.2</b> Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. For purposes of this requirement, “employee” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</p>	<p><b>9.2.a</b> Review processes and procedures for assigning badges to employees, and visitors, and verify these processes include the following:</p> <ul style="list-style-type: none"> <li>• Granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges</li> <li>• Limited access to badge system</li> </ul>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
	<p><b>9.2.b</b> Observe people within the facility to verify that it is easy to distinguish between employees and visitors.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.3</b> Make sure all visitors are handled as follows:</p>	<p><b>9.3</b> Verify that employee/visitor controls are in place as follows:</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.3.1</b> Authorized before entering areas where cardholder data is processed or maintained</p>	<p><b>9.3.1</b> Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.3.2</b> Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee</p>	<p><b>9.3.2</b> Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outside and that visitor badges expire.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>

### 3. Details about Reviewed Environment

<p><b>9.3.3</b> Asked to surrender the physical token before leaving the facility or at the date of expiration</p>	<p><b>9.3.3</b> Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.4</b> Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.</p>	<p><b>9.4.a</b> 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.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
	<p><b>9.4.b</b> Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.5</b> 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.</p>	<p><b>9.5</b> Verify that the storage location is reviewed at least annually to determine that back-up media storage is secure.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.6</b> Physically secure all paper and electronic media that contain cardholder data.</p>	<p><b>9.6</b> Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media (including computers, removable electronic media, networking, and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes).</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.7</b> Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:</p>	<p><b>9.7</b> Verify that a policy exists to control distribution of media containing cardholder data, and that the policy covers all distributed media including that distributed to individuals.</p>	<p>N/A – Security Policy/Procedures (Physical Security/Data Classification)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.7.1</b> Classify the media so it can be identified as confidential.</p>	<p><b>9.7.1</b> Verify that all media is classified so that it can be identified as "confidential."</p>	<p>N/A – Security Policy/Procedures (Physical Security/Data Classification)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>

<b>9.7.2</b> Send the media by secured courier or other delivery method that can be accurately tracked.	<b>9.7.2</b> 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/Data Classification)	Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<b>9.8</b> Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).	<b>9.8</b> Select a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization.	N/A – Security Policy/Procedures (Physical Security)	Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<b>9.9</b> Maintain strict control over the storage and accessibility of media that contains cardholder data.	<b>9.9</b> Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.	N/A – Security Policy/Procedures (Physical Security)	Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<b>9.9.1</b> Properly maintain inventory logs of all media and conduct media inventories at least annually.	<b>9.9.1</b> 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)	Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
<b>9.10</b> Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	<b>9.10</b> Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:	N/A – Security Policy/Procedures (Physical Security)	Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.

<p><b>9.10.1</b> Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.</p>	<p><b>9.10.1.a</b> Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
	<p><b>9.10.1.b</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.</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p><b>9.10.2</b> Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.</p>	<p><b>9.10.2</b> 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).</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>	<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>

## 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 without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
<p><b>10.1</b> Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</p>	<p><b>10.1</b> Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.</p>	<p>Verizon Business confirmed through interviews and review of configured log settings, as well as review of the audit trail, that audit trails are enabled and active for the following components within the PCI Solution for Retail environment:</p> <ul style="list-style-type: none"> <li>• ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (direct ssh access) <ul style="list-style-type: none"> <li>– AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>– CiscoWorks (LMS) – for configuration management (non-security related) – (wireless logs not sent to LMS)</li> <li>– CSM (security alerts (e.g. firewall logs, IDS alerts, etc) sent from devices to CSM are forwarded to CS-MARS)</li> <li>– CiscoWorks NCM (configuration changes, policy/standards violations)</li> </ul> </li> <li>• Cisco ACS <ul style="list-style-type: none"> <li>– Local and AD authentication logs (auth requests forwarded to AD)</li> <li>– Local audit trail for ACS management</li> </ul> </li> <li>• CSM (Cisco Security Manager) <ul style="list-style-type: none"> <li>– AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>– Local audit trail for CSM management</li> </ul> </li> <li>• -CSA (Cisco Security Agent) Manager <ul style="list-style-type: none"> <li>– AD authentication logs (authentication requests sent directly to AD).</li> <li>– All CSA logs, alerts/events sent to CSA manager</li> <li>– Local audit trail for CSA management</li> </ul> </li> <li>• CS-MARS <ul style="list-style-type: none"> <li>– Local authentication logs (no ACS or AD authentication available)</li> <li>– CSA logging/alerts, CSM security events (firewall logs (ASAs and ISRs), IDS/IPS alerts)</li> <li>– Local audit trail for CS-MARS</li> </ul> </li> <li>• WCS (Wireless Console Server) <ul style="list-style-type: none"> <li>– Local authentication</li> <li>– Local audit trail for WCS management and wireless configuration changes</li> </ul> </li> <li>• CiscoWorks (LMS) <ul style="list-style-type: none"> <li>– AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>– ISR (router) and switch configuration management logs</li> <li>– Local audit trail for LMS management</li> </ul> </li> </ul>		<p><b>Note:</b> WCS audit trail exists for authentication and administrative access; however, the audit trail is difficult to follow and could require significant time, including experienced Cisco support to fully understand and piece together the audit trail.</p>

		<ul style="list-style-type: none"> <li>• CiscoWorks NCM             <ul style="list-style-type: none"> <li>- AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>- Audit trail of network device configuration changes (date and time of change, who made the change, and lines of configuration changed).</li> <li>- Local audit trail for NCM management</li> </ul> </li> <li>• Cisco ASDM             <ul style="list-style-type: none"> <li>- AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>- ASA firewall configuration changes and IDS/IPS alerts sent to CS-MARS.</li> </ul> </li> <li>• Cisco IDM             <ul style="list-style-type: none"> <li>- IDM local auth logs and local configuration changes.</li> </ul> </li> <li>• Cisco ACE XML Gateway             <ul style="list-style-type: none"> <li>- AD auth logs (Cisco ACS auth requests forwarded to AD).</li> <li>- Local audit trail for ACE XML Gateway management.</li> </ul> </li> <li>• RSA SecurID             <ul style="list-style-type: none"> <li>- RSA SecurID access logged through RSA Authentication Manager.</li> <li>- RSA SecurID logs captured by RSA enVision for reporting, alerting, and long-term storage.</li> </ul> </li> <li>• RSA Authentication Manager             <ul style="list-style-type: none"> <li>- RSA SecurID authentication attempts</li> <li>- Local audit trail for RSA Authentication Manager administrative access/mgmt.</li> <li>- Audit log SFTP'd to RSA enVision every 60 minutes for reporting, alerting, and long-term storage.</li> </ul> </li> <li>• RSA Access Manager             <ul style="list-style-type: none"> <li>- RSA Key Manager authentication logs</li> <li>- Local audit trail for RSA Access Manager access/management.</li> </ul> </li> <li>• RSA File Security Manager (RSA File Security Manager)             <ul style="list-style-type: none"> <li>- Local/AD auth logs (access to server)</li> <li>- CSA (Monitors and logs RSA File Security Manager binary use)</li> <li>- Access to RSA File Security Manager protected resources (e.g. access to cardholder data)</li> <li>- Local audit trail for RSA File Security Manager access/management.</li> </ul> </li> </ul>		
--	--	--	--	--

		<ul style="list-style-type: none"> <li>• RSA Key Manager                             <ul style="list-style-type: none"> <li>- Local/AD auth logs (access to server)</li> <li>- CSA (Monitors and logs Key Manager binary use)</li> <li>- Key Material requests</li> <li>- Local audit trail for Key Manager access/management.</li> </ul> </li> <li>• RSA enVision                             <ul style="list-style-type: none"> <li>- RSA local/AD auth logs</li> <li>- Local audit trail for RSA enVision access/management.</li> <li>- Local audit trail for RSA enVision log repository access.</li> <li>- RSA SecurID access logs (SFTP'd from RSA Authentication Manager every 60 minutes).</li> </ul> </li> <li>• NCR ACS Server                             <ul style="list-style-type: none"> <li>- Local/AD logs for server access</li> <li>- CSA (Monitors and logs NCR ACS binary use and access to NCR ACS application log files)</li> <li>- Local audit trail for NCR ACS access/management.</li> </ul> </li> </ul>		
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 confirmed the following log access to cardholder data within the Cisco's PCI Solution for Retail environment: <ul style="list-style-type: none"> <li>• NCR ACS (logs to EFT log file and Transaction Log)</li> <li>• RSA File Security Manager (logs access to cardholder data protected by RSA File Security Manager)</li> <li>• RSA Key Manager (logs key material requests (necessary for decryption of cardholder data))</li> <li>• Cisco CSA (installed on all Windows servers within the PCI Solution for Retail environment and configured to monitor and log use of NCR ACS application binaries and log files. Only encrypted cardholder data is accessible within NCR application log files. These files have been configured through Cisco CSA to only allow necessary process and administrative accounts access. Only masked data is accessible through the NCR ACS application.)</li> </ul>		

<p><b>10.2.2</b>All actions taken by any individual with root or administrative privileges</p>	<p><b>10.2.2</b>Verify actions taken by any individual with root or administrative privileges is logged.</p>	<p>Verizon Business reviewed audit log configurations to confirm administrative actions are logged for the following:</p> <ul style="list-style-type: none"> <li>• Management of ASA firewalls, FWSMs, ISRs, routers, IDSM2, switches (ASDM, SDM, CSM, or SSH (forwarded to CS-MARS), CiscoWorks (LMS))</li> <li>• CS-MARS administration (CS-MARS audit trail)</li> <li>• ACS administration (CSA and local ACS audit trail)</li> <li>• CSA administration (CSA and local CSA audit trail)</li> <li>• CiscoWorks administration (LMS) (CSA and local LMS audit trail)</li> <li>• Wireless controllers (WCS logs)</li> <li>• WCS (CSA and local WCS audit trail – Administrative changes to WCS are logged to the audit trail, but difficult to determine the details of the change)</li> <li>• CSM administration (CSA and local CSM audit trail)</li> <li>• NCM administration (CSA and NCM audit trail)</li> <li>• Cisco ACE XML Gateway (local ACE XML Gateway audit trail)</li> <li>• Cisco IDM (local IDM audit trail)</li> <li>• RSA Authentication Manager (CSA, local RSA Authentication Manager audit trail, RSA enVision (SFTP'd from RSA Authentication Manager every 60 minutes))</li> <li>• RSA Access Manager (CSA, local RSA Access Manager audit trail)</li> <li>• RSA Key Manager (local audit trail for Key Manager administration)</li> <li>• RSA enVision (local audit trail for enVision administration)</li> <li>• NCR ACS Server (local EFT and Transaction Log files)</li> </ul> <p><b>Note:</b> Reference to CSA is for administrative changes on Windows host OS for each application running on Windows.</p>	<p>The following have limited audit trails, related to administrative actions:</p> <ul style="list-style-type: none"> <li>• RSA File Security Manager (not all administrative actions are logged - to be addressed in FSM v2.2 release)</li> </ul>	<p><b>Note:</b> Wireless audit trail exists for authentication and administrative access; however, the audit trail is difficult to follow and could require significant time, including experienced Cisco support to fully understand and piece together the audit trail.</p>
--	--	--	--	---



<p><b>10.2.3</b> Access to all audit trails</p>	<p><b>10.2.3</b> Verify access to all audit trails is logged.</p>	<p>Verizon Business observed CSA Manager policies, log directories and log files monitored by CSA, and CSA event logs generated upon unauthorized access of audit log files and directories, to determine access to the following audit trails is being logged:</p> <ul style="list-style-type: none"> <li>• ACS, CiscoWorks (LMS, NCM), CSA Manager, CSM, WCS Manager, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, NCR ACS: <ul style="list-style-type: none"> <li>– Live log directory and files (CSA is configured to allow application services to write/delete/modify files in the live log directory and rotate (archive) log files to an archive directory. All other users and processes are restricted from accessing, modifying, or deleting files within the live log directories. This prevents users from accessing the audit trail outside of the application (ACS, CiscoWorks (LMS, NCM), WCS, CSM, CSA console, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, NCR ACS). Cisco created a custom archive script which is run from a central backup server and copies all audit logs to a central backup server, where additional CSA protection can be applied. The archive directories are monitored to protect all processes and users from deleting or modifying files written to the archive directory, other than the backup user account which copies files to this directory (necessary to copy files and delete files older than 1 year).</li> </ul> </li> <li>• CS-MARS (appliance server, which does not support CSA) <ul style="list-style-type: none"> <li>– Audit log files backed up daily to an NFS backup server are monitored by CSA and all processes and users (except the application processes responsible for writing data to the NFS server) are prohibited from modifying or deleting files from this directory.</li> </ul> </li> <li>• RSA enVision (not monitored by CSA, because log files are stored within a proprietary database) <ul style="list-style-type: none"> <li>– Access to application is restricted to least privilege, role-based accounts, and logged</li> <li>– Details on reports run/viewed is logged</li> </ul> </li> </ul> <p>Verizon Business observed unauthorized attempts to access the audit trail, outside the application. CSA alerts were generated, sent to the CS-MARS central server, and an email alert was sent to the administrator.</p>	<p><b>Note:</b> Management consoles reviewed did not log access to audit trails, without CSA monitoring of audit logs. Cisco used a custom archive/backup method to copy the audit trail to a central backup server. Cisco has inserted the script within the Appendix of their implementation guide.</p>
---	---	--	---

<p><b>10.2.4</b>Invalid logical access attempts</p>	<p><b>10.2.4</b>Verify invalid logical access attempts are logged.</p>	<p>Verizon Business confirmed that invalid logical access attempts are logged for the following:</p> <ul style="list-style-type: none"> <li>• All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers</li> <li>• Access to CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, CSM, and ACE XML Gateway, IDM</li> <li>• Access to RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager</li> <li>• NCR ACS Server</li> </ul>		
<p><b>10.2.5</b>Use of identification and authentication mechanisms</p>	<p><b>10.2.5</b>Verify use of identification and authentication mechanisms is logged.</p>	<p>Verizon Business confirmed that userID for authentication is logged for authentication to the following:</p> <ul style="list-style-type: none"> <li>• All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers</li> <li>• CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, CSM, ACE XML Gateway, IDM</li> <li>• RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager</li> <li>• NCR ACS Server</li> </ul>		
<p><b>10.2.6</b>Initialization of the audit logs</p>	<p><b>10.2.6</b>Verify initialization of audit logs is logged.</p>	<p>Verizon Business confirmed that RSA enVision does not provide capabilities to delete the audit trail through the application. See 10.2.3 (CSA protection for audit trail access applies to initialization of audit trail)</p>		<p><a href="#">See 10.2.3 (CSA protection for audit trail access applies to initialization of audit trail)</a></p>
<p><b>10.2.7</b>Creation and deletion of system-level objects</p>	<p><b>10.2.7</b>Verify creation and deletion of system level objects are logged.</p>	<p>Verizon Business confirmed CSA is installed on all Windows servers within the PCI Solution for Retail environment and is configured to capture deletion of system level objects. Additionally, CiscoWorks (LMS, NCM), and CSM capture all administrative actions for ASA firewalls, FWSMs, ISRs, IDSM2 and switches.</p>		
<p><b>10.3</b>Record at least the following audit trail entries for all system components for each event:</p>	<p><b>10.3</b> Through interviews and observation, for each auditable event (from 10.2), perform the following:</p>			

10.3.1 User identification	10.3.1 Verify user identification is included in log entries.	<p>Verizon Business confirmed userID is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers</li> <li>CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM.</li> <li>RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager</li> <li>NCR ACS Server</li> </ul>		
10.3.2 Type of event	10.3.2 Verify type of event is included in log entries.	<p>Verizon Business confirmed event type is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes)</li> <li>CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (contained within local audit trails)</li> <li>CSA generated logs and alerts contain event type within each record.</li> <li>ACS and AD contain event type within each authentication record.</li> <li>RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records)</li> <li>NCR ACS Server (contained within EFT and Transaction Log files)</li> </ul>		
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.	<p>Verizon Business confirmed date and time stamp is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes)</li> <li>CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (date and time stamp contained within local audit trail records)</li> <li>CSA generated logs and alerts contain a date and time stamp within each record.</li> <li>ACS and AD contain date and time stamp for each authentication record.</li> <li>RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records)</li> <li>NCR ACS Server (contained within EFT and Transaction Log files)</li> </ul>		

<p><b>10.3.4</b>Success or failure indication</p>	<p><b>10.3.4</b>Verify success or failure indication is included in log entries.</p>	<p>Verizon Business confirmed “success or failure” indication is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>• All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – audit events would indicate a successful change to the configuration. Failed actions based on insufficient permissions would be logged in the ACS audit trail.)</li> <li>• CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (success or failure is evident based on event type and/or event detail).</li> <li>• “Success” or “Failure” indication is evident within CSA generated logs and alerts based on the event type.</li> <li>• ACS and AD logs contain success or failure indication for each authentication record.</li> <li>• RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (evident based on details within audit trail records)</li> <li>• NCR ACS Server (evident based on details within audit trail records)</li> </ul>		
<p><b>10.3.5</b>Origination of event</p>	<p><b>10.3.5</b>Verify origination of event is included in log entries.</p>	<p>Verizon Business confirmed “origination of event” is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>• All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – security and syslog messages indicate originating device.)</li> <li>• CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (local audit trail indicates whether event is locally generated or sent from managed device).</li> <li>• CSA generated logs and alerts indicate originating host.</li> <li>• ACS and AD logs contain originating system for each authentication record.</li> <li>• RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records)</li> <li>• NCR ACS Server (all records are local to system)</li> </ul>		

<p><b>10.3.6</b> Identity or name of affected data, system component, or resource</p>	<p><b>10.3.6</b> Verify identity or name of affected data, system component, or resources is included in log entries.</p>	<p>Verizon Business confirmed “name of affected data, system component, or resource” is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> <li>• All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – security and syslog messages indicate specific configuration changes being made.)</li> <li>• CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (local audit trail indicates affected data or resource through event type).</li> <li>• CSA generated logs and alerts indicate detailed information on affected data.</li> <li>• RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (evident based on details within audit trail records)</li> <li>• NCR ACS Server (evident based on details within audit trail records)</li> </ul>		
<p><b>10.4</b> Synchronize all critical system clocks and times.</p>	<p><b>10.4</b> Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:</p>	<p>Verizon Business reviewed device configurations to confirm management consoles, ACE XML Gateway, ASA firewalls, FWSMs, IDSM2, ISR routers, switches, and wireless devices synchronize system clocks as follows:</p>		
	<p><b>10.4.a</b> Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.</p>	<p>NTP is used for all time synchronization on all system components reviewed.</p>		

<p><b>10.4.b</b> Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]</p>	<p>Verizon Business reviewed network device configurations and Windows registry settings to confirm all servers and network devices within the PCI Solution for Retail environment point to at least two internal NTP servers.</p>		
<p><b>10.4.c</b> Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (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 NTP service (to prevent unauthorized use of internal time servers). See <a href="http://www.ntp.org">www.ntp.org</a> for more information</p>	<p>Verizon Business reviewed vendor documentation for the NTP appliances. Internal NTP appliances point to a pool of IP addresses under pool.ntp.org and time.nist.gov. Internal NTP servers do not receive NTP updates, but poll external servers for time updates.</p>		

<b>10.5</b> Secure audit trails so they cannot be altered.	<b>10.5</b> Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
<b>10.5.1</b> Limit viewing of audit trails to those with a job-related need.	<b>10.5.1</b> Verify that only individuals who have a job-related need can view audit trail files.	Verizon Business confirmed CS-MARS and RSA enVision, as well as all back-end management consoles, are segmented behind multiple firewalls within the data center environment. All firewalls have been configured to only allow necessary inbound and outbound traffic.  See 10.2.3 for additional audit trail access details.		<a href="#">See 10.2.3</a>
<b>10.5.2</b> Protect audit trail files from unauthorized modifications.	<b>10.5.2</b> Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	See 10.2.3/10.5.1 above		<a href="#">See 10.2.3</a>
<b>10.5.3</b> Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	<b>10.5.3</b> Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	Verizon Business confirmed centrally stored audit logs within CS-MARS are archived once an hour and sent to a central NFS server running CSA software.  CiscoWorks (LMS) is archiving audit trail once a day. (See 10.2.3 for additional details of audit trail archiving)  RSA enVision centrally stores RSA SecurID log records (sent every 60 minutes from RSA Authentication Manager).		<a href="#">See 10.2.3</a>
<b>10.5.4</b> Write logs for external-facing technologies onto a log server on the internal LAN.	<b>10.5.4</b> 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 confirmed wireless logs and firewall logs are sent to WCS and CS-MARS central servers.		

<p><b>10.5.5</b> 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).</p>	<p><b>10.5.5</b> 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.</p>	<p>Cisco Security Agent (CSA) software is used to monitor and protect access to audit trail files, and alert on unauthorized attempts to modify the audit trail (only application services responsible for writing log data can write/modify/delete the audit trail). Cisco has created an additional backup script to copy the audit trail to a central backup server, where CSA protection has been applied to eliminate all access, modification, and deletion, except for the account responsible for backing up the audit trail (see 10.2.3 for additional details).</p> <p>RSA enVision’s proprietary database uses 32-bit checksums for log record integrity, in addition to its write-once, read-many design. Audit records cannot be modified through the application.</p>	
<p><b>10.6</b> 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).</p> <p>Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6</p>	<p><b>10.6.a</b> 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.</p>	<p>Verizon Business confirmed the use of CS-MARS, RSA enVision, and CSA software, which perform correlation and analysis of system events, and alert on those warranting immediate action.</p> <p><b>Note:</b> Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions (responsibility of merchant / service provider)</p>	<p><b>Note:</b> Although manual log review, escalation, and follow-up procedures would be the responsibility of the merchant / service provider, automated log correlation, analysis, and alerting is the most efficient way to stay on top of copious amounts of log data.</p>
	<p><b>10.6.b</b> Through observation and interviews, verify that regular log reviews are performed for all system components.</p>	<p>See 10.6.a above.</p>	<p>Interviews to be conducted with each merchant / service provider.</p>



<p><b>10.7</b> 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).</p>	<p><b>10.7.a</b> 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.</p>	<p>N/A – Security Policy (Data Retention)</p>	<p>Retention policy and procedure documentation is the responsibility of the merchant / service provider.</p>
	<p><b>10.7.b</b> Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.</p>	<p>Verizon Business reviewed online logs and audit trail archive methods within the PCI Solution for Retail environment to confirm audit trails can be retained for at least one year, with at least three months available online.</p>	<p><b>Note:</b> Due to the nature of the lab environment reviewed, and the recent addition to some components within the environment, archive logs were not available for the full 90 days, for all components; however, sufficient disk space is available to accommodate this logging. Additionally, log retention is directly dependant on the amount of logging within the environment. Proper sizing, based on expected traffic patterns, is critical to ensuring sufficient space is available for online logs.</p>

### 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	Target Date/ Comments
<p><b>11.1</b> Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.</p>	<p><b>11.1.a</b> Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.</p>	<p>Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.</p>		
	<p><b>11.1.b</b> If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.</p>			<p>Wireless IDS/IPS is a new (optional) control within the PCI DSS v1.2 standard. The wireless infrastructure assessed as part of phase 2 was not assessed to determine wireless IDS/IPS capabilities.</p>
	<p><b>11.1 c</b> Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant/ service provider</p>
<p><b>11.2</b> 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).</p> <p><i>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.</i></p>	<p><b>11.2.a</b> Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained.</p> <p>Note: External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.</p>	<p>N/A – Internal quarterly scanning</p>		<p>Responsibility of merchant/ service provider.</p>

	<p><b>11.2.b</b> Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that:</p> <p>Four quarterly scans occurred in the most recent 12-month period;</p> <p>The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities);</p> <p>The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC.</p> <p>Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.</p>	N/A – Third party external, quarterly scanning		Responsibility of merchant/service provider.
	<p><b>11.2.c</b> Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.</p>	N/A – Third party external scanning / Internal scanning		Responsibility of merchant/service provider.

<p><b>11.3</b> 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:</p>	<p><b>11.3.a</b> 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. Verify that noted vulnerabilities were corrected and testing repeated.</p>	<p>N/A – Penetration Testing (at least annually)</p>	<p>Responsibility of merchant / service provider.</p> <p><b>Note:</b> Penetration testing needs to be conducted on internal and external system components (network devices, applications, and servers), which are “in scope” for PCI.</p>
	<p><b>11.3.b</b> Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).</p>	<p>N/A – Penetration Testing (at least annually)</p>	<p>Responsibility of merchant / service provider.</p> <p><b>Note:</b> Penetration testing is to be conducted by a qualified internal resource or qualified external third party. Internal resources should be independent from resources responsible for the systems being tested (e.g. should not be the network / system administrator).</p>
<p><b>11.3.1</b> Network-layer penetration tests</p>	<p><b>11.3.1</b> Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.</p>	<p>N/A – Penetration Testing (at least annually)</p>	<p>Responsibility of merchant / service provider.</p>
<p><b>11.3.2</b> Application-layer penetration tests</p>	<p><b>11.3.2</b> Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.</p>	<p>N/A – Penetration Testing (at least annually)</p>	<p>Responsibility of merchant / service provider.</p>

<p><b>11.4</b> Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.</p>	<p><b>11.4.a</b> Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored.</p>	<p>Verizon Business reviewed the PCI Solution for Retail environment, including device configurations and confirmed Cisco ASA firewalls (with integrated IDS/IPS), ISRs (with integrated IOS IDS), and IDSM-2 modules were configured with full IDS functionality. Verizon Business reviewed IDS placement within the retail and datacenter (Internet Edge, WAN edge, and core data center segments) networks, and confirmed that all critical traffic to, from, and within the PCI Solution for Retail environment would be subject to IDS monitoring. Cisco CSA (host-based IDS/IPS) is also used on critical POS servers and management consoles (e.g. CSM, CiscoWorks (LMS, NCM), CSA console, ACS, and WCS console).</p>		
	<p><b>11.4.b</b> Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.</p>	<p>Verizon Business confirmed IDS/IPS is in place and can be configured to monitor and alert personnel of suspected compromise.</p>		
	<p><b>11.4.c</b> Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.</p>	<p>Verizon Business confirmed ASA firewalls, FWSMs, ISRs, and IDSM-2 versions are running updated releases, and are configured to automatically update IDS/IPS signatures. CSA (host-based IDS/IPS) does not rely on signatures, but is behavioral based, eliminating the need to update signatures.</p>		

<p><b>11.5</b>Deploy file-integrity monitoring software 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.</p> <p><i>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).</i></p>	<p>Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities.</p> <p>Examples of files that should be monitored:</p> <ul style="list-style-type: none"> <li>• System executables</li> <li>• Application executables</li> <li>• Configuration and parameter files</li> <li>• Centrally stored, historical or archived, log and audit files</li> </ul>	<p>Verizon Business reviewed vendor documentation and observed Cisco Security Agent software in the PCI Solution for Retail environment. In addition to logging and alerting on critical file modification, CSA can also log and alert on attempted access, allowed or denied. Since the initial phase I review of CSA, CSA has been updated with new PCI rules, complete with critical OS files.</p>		
---	--	---	--	--

## Maintain an Information Security Policy

### Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
<p><b>12.1</b>Establish, publish, maintain, and disseminate a security policy that accomplishes the following:</p>	<p><b>12.1</b>Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).</p>	<p>N/A – Security Policy</p> <p><b>Note:</b> Verizon Business has assisted numerous merchants and service providers to create new and augment existing policies and procedures to meet PCI requirements.</p>		<p>Responsibility of merchant / service provider</p>

<b>12.1.1</b> Addresses all PCI DSS requirements.	<b>12.1.1</b> Verify that the policy addresses all PCI DSS requirements.	N/A – Security Policy		Responsibility of merchant / service provider
<b>12.1.2</b> Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	<b>12.1.2</b> Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.	N/A – Security Policy		Responsibility of merchant / service provider
<b>12.1.3</b> Includes a review at least once a year and updates when the environment changes.	<b>12.1.3</b> 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		Responsibility of merchant / service provider
<b>12.2</b> Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	<b>12.2.a</b> 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		Responsibility of merchant / service provider
<b>12.3</b> Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	<b>12.3</b> Obtain and examine the policy for critical employee-facing technologies and perform the following:			
<b>12.3.1</b> Explicit management approval	<b>12.3.1</b> Verify that the usage policies require explicit management approval to use the technologies.	N/A – Acceptable Use Policy		Responsibility of merchant / service provider
<b>12.3.2</b> Authentication for use of the technology	<b>12.3.2</b> 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		Responsibility of merchant / service provider

### 3. Details about Reviewed Environment

<b>12.3.3A</b> list of all such devices and personnel with access	<b>12.3.3</b> Verify that the usage policies require a list of all devices and personnel authorized to use the devices.	N/A – Acceptable Use Policy / Asset List		Responsibility of merchant / service provider
<b>12.3.4</b> Labeling of devices with owner, contact information, and purpose	<b>12.3.4</b> Verify that the usage policies require labeling of devices with owner, contact information, and purpose.	N/A – Acceptable Use Policy / Asset List		Responsibility of merchant / service provider
<b>12.3.5</b> Acceptable uses of the technology	<b>12.3.5</b> Verify that the usage policies require acceptable uses for the technology.	N/A – Acceptable Use Policy		Responsibility of merchant / service provider
<b>12.3.6</b> Acceptable network locations for the technologies	<b>12.3.6</b> Verify that the usage policies require acceptable network locations for the technology.	N/A – Acceptable Use Policy		Responsibility of merchant / service provider
<b>12.3.7</b> List of company-approved products	<b>12.3.7</b> Verify that the usage policies require a list of company-approved products.	N/A – Acceptable Use Policy		Responsibility of merchant / service provider
<b>12.3.8</b> Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	<b>12.3.8</b> 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		Responsibility of merchant / service provider
<b>12.3.9</b> Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	<b>12.3.9</b> Verify that the usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.	N/A – Acceptable Use / Remote Access Policy		Responsibility of merchant / service provider
<b>12.3.10</b> When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	<b>12.3.10</b> 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		Responsibility of merchant / service provider
<b>12.4</b> Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	<b>12.4</b> Verify that information security policies clearly define information security responsibilities for both employees and contractors.	N/A – Security Policy		Responsibility of merchant / service provider



<b>12.5</b> Assign to an individual or team the following information security management responsibilities:	<b>12.5</b> 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		Responsibility of merchant / service provider
<b>12.5.1</b> Establish, document, and distribute security policies and procedures.	<b>12.5.1</b> Verify that responsibility for creating and distributing security policies and procedures is formally assigned.	N/A – Security Policy		Responsibility of merchant / service provider
<b>12.5.2</b> Monitor and analyze security alerts and information, and distribute to appropriate personnel.	<b>12.5.2</b> 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)		Responsibility of merchant / service provider
<b>12.5.3</b> Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	<b>12.5.3</b> Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.	N/A – Security Policy (Incident Response)		Responsibility of merchant / service provider
<b>12.5.4</b> Administer user accounts, including additions, deletions, and modifications	<b>12.5.4</b> Verify that responsibility for administering user account and authentication management is formally assigned.	N/A – Security Policy (ID / Account management)		Responsibility of merchant / service provider
<b>12.5.5</b> Monitor and control all access to data.	<b>12.5.5</b> Verify that responsibility for monitoring and controlling all access to data is formally assigned.	N/A – Security Policy (Data Control / Monitoring)		Responsibility of merchant / service provider
<b>12.6</b> Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	<b>12.6.a</b> Verify the existence of a formal security awareness program for all employees.	N/A – Security Policy (Security Awareness)		Responsibility of merchant / service provider
	<b>12.6.b</b> Obtain and examine security awareness program procedures and documentation and perform the following:			

### 3. Details about Reviewed Environment

<p><b>12.6.1</b>Educate employees upon hire and at least annually.</p>	<p><b>12.6.1.a</b>Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, memos, web based training, meetings, and promotions).</p>	<p>N/A – Security Policy (Security Awareness)</p>		<p>Responsibility of merchant / service provider</p>
	<p><b>12.6.1.b</b>Verify that employees attend awareness training upon hire and at least annually.</p>	<p>N/A – Security Policy (Security Awareness)</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.6.2</b>Require employees to acknowledge at least annually that they have read and understood the company’s security policy and procedures.</p>	<p><b>12.6.2</b>Verify that the security awareness program requires employees to acknowledge (for example, in writing or electronically) at least annually that they have read and understand the company’s information security policy.</p>	<p>N/A – Security Policy (Security Awareness)</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.7</b>Screen potential employees (see definition of “employee” at 9.2 above) prior to hire to minimize the risk of attacks from internal sources.</p> <p>For those employees 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.</p>	<p><b>12.7</b>Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on employees prior to hire who will have access to cardholder data or the cardholder data environment. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)</p>	<p>N/A – Security Policy (Background Checks)</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.8</b>If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:</p>	<p><b>12.8</b>If the entity being assessed 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:</p>			
<p><b>12.8.1</b>Maintain a list of service providers.</p>	<p><b>12.8.1</b>Verify that a list of service providers is maintained.</p>	<p>N/A – Connected Entity List (List of Service Providers with whom cardholder data is shared)</p>		<p>Responsibility of merchant / service provider</p>

<b>12.8.2</b> Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	<b>12.8.2</b> Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.	N/A – Third party contracts		Responsibility of merchant / service provider
<b>12.8.3</b> Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	<b>12.8.3</b> 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		Responsibility of merchant / service provider
<b>12.8.4</b> Maintain a program to monitor service providers' PCI DSS compliance status.	<b>12.8.4</b> Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.	N/A – Policies and Procedures for sharing cardholder data with third parties / Service Providers		Responsibility of merchant / service provider
<b>12.9</b> Implement an incident response plan. Be prepared to respond immediately to a system breach.	<b>12.9</b> Obtain and examine the Incident Response Plan and related procedures and perform the following:			

<p><b>12.9.1</b>Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:</p> <ul style="list-style-type: none"> <li>• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum</li> <li>• Specific incident response procedures</li> <li>• Business recovery and continuity procedures</li> <li>• Data back-up processes</li> <li>• Analysis of legal requirements for reporting compromises</li> <li>• Coverage and responses of all critical system components</li> <li>• Reference or inclusion of incident response procedures from the payment brands</li> </ul>	<p><b>12.9.1</b>Verify that the Incident Response Plan includes:</p> <ul style="list-style-type: none"> <li>• Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum</li> <li>• Specific incident response procedures,</li> <li>• Business recovery and continuity procedures,</li> <li>• Data back-up processes</li> <li>• 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)</li> <li>• Coverage and responses for all critical system components</li> <li>• Reference or inclusion of incident response procedures from the payment brands</li> </ul>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.9.2</b>Test the plan at least annually.</p>	<p><b>12.9.2</b>Verify that the plan is tested at least annually.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.9.3</b>Designate specific personnel to be available on a 24/7 basis to respond to alerts.</p>	<p><b>12.9.3</b>Verify through observation and review of policies, that there is 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.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.9.4</b>Provide appropriate training to staff with security breach response responsibilities.</p>	<p><b>12.9.4</b>Verify through observation and review of policies that staff with security breach responsibilities are periodically trained.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>

<p><b>12.9.5</b> Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.</p>	<p><b>12.9.5</b> 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.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>
<p><b>12.9.6</b> Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.</p>	<p><b>12.9.6</b> 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.</p>	<p>N/A – Incident Response policy and procedures</p>		<p>Responsibility of merchant / service provider</p>

