



Meeting PCI Compliance



Ricky Elias

Security Architect

Advanced Technology (Security)

relias@cisco.com

The Payment Card Industry (PCI) Data Security Standard

- Published January 2005
- Impacts ALL who **process, transmit, or store** cardholder data
- Also applies to 3rd-party hosting companies, information storage companies, etc.
- Monthly fines ranging from \$5,000 to \$100,000 for missed deadlines
- **Has global reach**

Theater	Level 1	Level 2	Level 3
US	SEP 2007	DEC 2007	DEC 2008
Western Europe	Negotiated individually	MAR-DEC 2008	MAR-DEC 2008
Asia	DEC 2009	DEC 2009	DEC 2009
Canada	2008 TBD	2008 TBD	2008 TBD
Latin American CEMEA	Not Published yet		

Compliance Requirements Global Alignment

11 November 2008 | Singapore

Visa Sets Global PCI DSS Deadlines

Data Security Compliance Requirements Aligned Across Visa Regions

Effective Date	Globally Aligned Mandate
February 1, 2009	Effective date for globally aligned Service Provider level definitions
September 30, 2009	Acquirers must attest that Level 1 and 2 merchants do not retain prohibited payment card data subsequent to authorization of a transaction
September 30, 2010	PCI DSS compliance validation deadline for Level 1 merchants

http://www.visa-asia.com/ap/sea/mediacenter/pressrelease/NR_SGP_111108.shtml

VISA PCI Categories

Level/Tier	Merchant Criteria	Requirement
1	Over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region	Annual Report on Compliance (ROC) Quarterly Network Scan Attestation of Compliance
2	1 million to 6 million Visa transactions annually (all channels)	Annual Self-Assessment Quarterly Network Scan Attestation of Compliance
3	20,000 to 1 million Visa e-commerce transactions annually	Annual Self-Assessment Quarterly Network Scan Attestation of Compliance
4	Less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions	Annual Self-Assessment Quarterly Network Scan Compliance validation requirements set by acquirer

Source: VISA http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais_how.shtml

PCI Standards Update

- New PCI Self-Assessment Questionnaires (SAQ) release
 - One SAQ → four SAQs to reach more merchants
- PCI DSS version 1.2 released October 2008
- Two Information Supplements released April 22, 2008
 - 11.3 Penetration testing
 - 6.6 Web Application Firewall
- List of [Qualified Security Assessors](#) (QSA) continuously updated
- List of [Approved Scan Vendors](#) (ASV) continuously updated

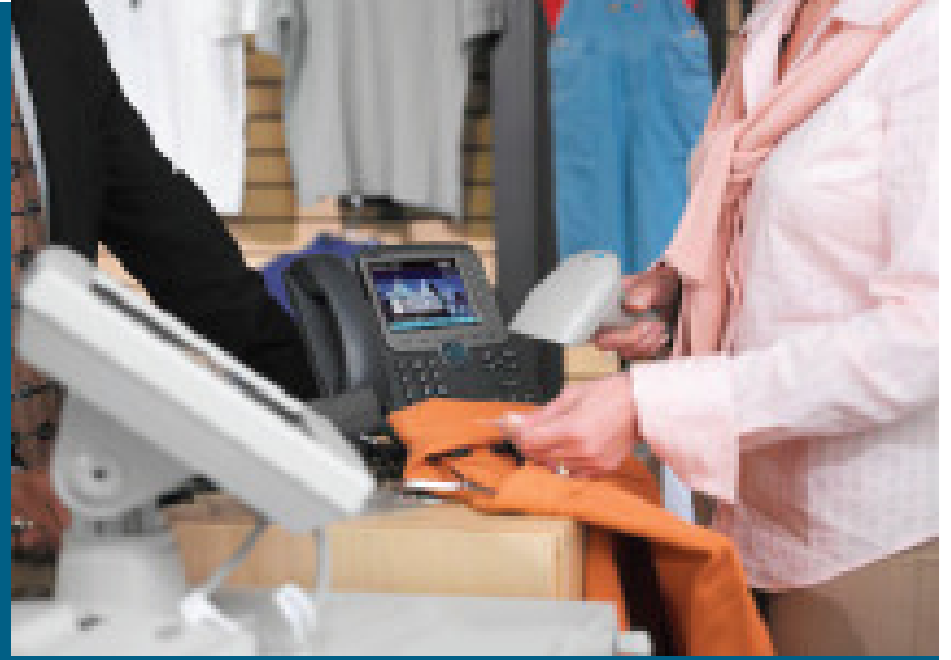
Addressing the Twelve Requirements of PCI DSS

	PCI Data Security Standard Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security requirements
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security

PCI Compliance Failure Rates

PCI Data Security Standard Requirements		Percentage of Assessment Failures*
Build and Maintain a Secure Network	1. Install & maintain a firewall configuration to protect data	66%
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	62%
Protect Cardholder Data	3. Protect stored data	79%
	4. Encrypt transmission of cardholder data and sensitive information across public networks	45%
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software	
	6. Develop and maintain secure systems and applications	56%
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know	
	8. Assign a unique ID to each person with computer access	71%
	9. Restrict physical access to cardholder data	59%
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	71%
	11. Regularly test security systems and processes	74%
Maintain an Information Security Policy	12. Maintain a policy that addresses information security	60%

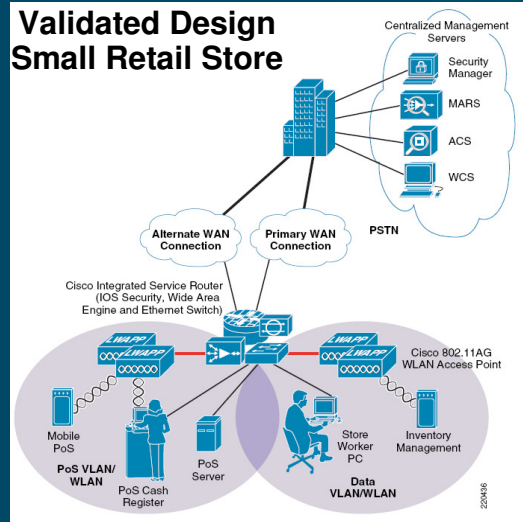
Applying Cisco Solutions to PCI



Cisco PCI Validated Architectures

Cisco Validated Design includes:

- Recommended architectures for networks, payment data at rest and data in-transit
- Testing in a simulated retail enterprise which include POS terminals, application servers, wireless devices, Internet connection and security systems
- Configuration, monitoring, and authentication management systems
- Architectural design guidance and audit review provided by PCI audit and remediation partners



PCI Audit Partner:

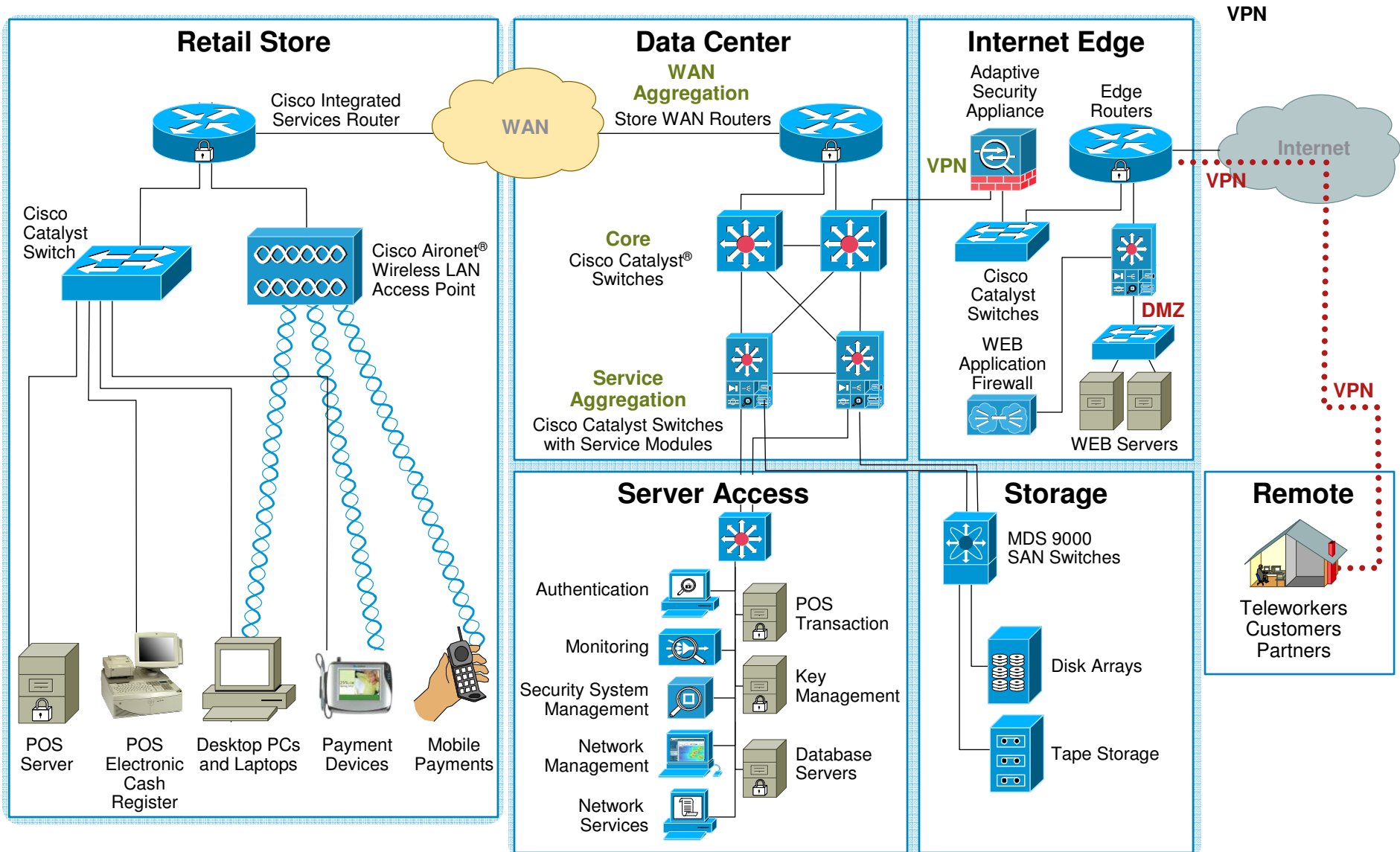


Retail Solution Partners:



PCI Solution for Retail

End-to-End Architecture



PCI Requirement 2

Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- Change vendor supplied defaults
- Wireless: Change wireless vendor defaults, disable SSID broadcasts, use WPA/WPA2
- Configuration standards for all system components
- Implement one primary function per server
- Disable all unnecessary and insecure services and protocols



PCI Requirement 2.1 for Wireless

- Verify that the Cisco Controller is, by default, configured for administrative restriction and AAA authentication for administrative users
- Verify that no default SSID is enabled on the WLC
- Disable/remove default SNMP strings of “public/private”
- Create new community strings
- Verify that default community strings are no longer accessible
- Configure administrative user either via initial controller setup script or via CLI
- Configure wireless system for WPA authentication
- Disable SSID Broadcast

PCI Requirement 3

Protect Stored Data

- Keep cardholder data storage to a minimum
- Do not store the full contents of any track from the magnetic stripe (also called full track, track, track1, track 2 and magnetic stripe data), card-validation code or value, PIN
- Mask PAN when displayed, and render it unreadable when stored (hashed indexes, truncation, index tokens and pads, strong cryptography), disk encryption
- Document and implement key management processes



Protect Stored Data: From What?

- Cisco Security Agent (CSA) protects from:
 - Copying cardholder information to removable media (USB sticks, CD ROMs, etc.)
 - Copying cardholder information to different file formats
 - Printing cardholder information
 - Saving information to a local machine
- Plus typical worm/virus protection (think e-commerce)

PCI Requirement 4

Encrypt Transmission of Cardholder Data Across Open, Public Networks

- Use SSL/TLS or IPsec, WPA for wireless
- If using WEP:
 - Use with a minimum 104-bit encryption key and 24 bit-initialization value
 - Use **only** in conjunction with WPA/WPA2, VPN or SSL/TLS
 - Rotate shared WEP keys quarterly (or automatically)
 - Restrict access based on MAC address
- Never send unencrypted PANs by e-mail



IronPort: PCI Compliance over Email

Automatic Detection and Encryption of Credit Card Info

- Comprehensive Scanning for Cardholder Info
- Integrated Encryption and Remediation
- Auditable Reporting



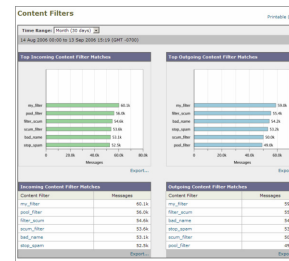
Comprehensive Detection:

- Credit Card Smart Identifier
- Preloaded PCI Lexicons Dictionary
- Embedded Attachment Scanning

Enable Smart Identifiers	Weight
<input checked="" type="checkbox"/> Credit Card Numbers	10
<input type="checkbox"/> Social Security Numbers	1

Integrated Remediation:

- Universal Message Encryption
- Quarantine, Archive Capabilities
- Notifications
- Reporting



“IronPort meets PCI compliance requirements in an **easy to administer, transparent manner.**”

—Brian Burke, Director, Secure Content, IDC

“IronPort has provided customers with an **easy to deploy, use, and manage PCI compliance solution for email.**”

—Barry Johnson, Director, Risk Mitigation, IGXGlobal


Audit Process Assessment and ROC

- The QSA's Assessment report is the written response to the audit process.

For areas that do not pass, QSA will recommend **compensating controls**

Remediation services are typically required after the audit.

- After audit and remediation, the retailer can submit their **Report of Compliance** for review by a PCI Company (e.g., Visa, MasterCard) for final approval.




**Cybertrust Assessment:
Cisco PCI Solution for Retail**

Security Audit Procedures

PCI DSS - Version 1.1
Release: September 2006

Report Date: 01/29/2007



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 into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet 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
1.1 Establish firewall configuration standards that include the following:	1.1 Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	1.1.1 Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant/ service provider.
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks	Cisco provided a current network diagram, which documents all connections to the cardholder data, applicable to the reference architecture environment, including wireless networks.		
	1.1.2.b. Verify that the diagram is kept current	Current diagrams were provided for each PCI Solution for Retail environment (e.g. Small, medium,		Note: Since each network environment will be unique to the

Cybertrust, Inc. Security Audit Procedures v 1.1 Cisco Systems, Inc. 12

More Information

- Cisco Compliance information

<http://www.cisco.com/go/compliance>

<http://www.cisco.com/go/retail>

- VISA Cardholder Information Security Program

http://usa.visa.com/merchants/risk_management/cisp.html

- MasterCard PCI Merchant Education

<http://www.mastercard.com/us/sdp/education/pci%20merchant%20education%20program.html>

- PCI Security Standards Council

<https://www.pcisecuritystandards.org/>

