

PCI DSS 3.0 Update: A Cisco and Verizon Perspective



What You Will Learn

Since 2007, Cisco and Verizon have partnered to offer Payment Card Industry (PCI) compliance guidance. The resulting Cisco® Compliance Solution for PCI was developed to implement guidance in specific Cisco laboratory configurations that undergo Verizon Qualified Security Assessor (QSA) assessment. With the release of PCI Data Security Standard (DSS) 3.0¹, there are questions that Cisco customers naturally ask. What are the significant changes from version 2.0 to 3.0? How do they affect the existing Cisco Compliance Solution for PCI? In this document, you'll learn:

- How PCI DSS 3.0 affects the scoping, vendor equipment assessment, and enterprise architecture of existing Cisco Compliance Solution for PCI implementations
- The significant changes between PCI DSS 2.0 and 3.0

Cisco Compliance Solution for PCI

The Cisco Compliance Solution for PCI provides enterprise guidance and component-level configurations:

- **Enterprise architecture:** The solution uses reference architecture to validate compliance guidance. The reference architecture consists of multiple-size branch offices, WANs, the data center, and Internet edge technology. It details the security and respective compliance controls as credit card transactions occur at the branch location and flow throughout the enterprise, where they exit to the acquiring banks. Cisco has compliance laboratories on its San Jose campus in Building 17s.

Assessment: The architecture sections of the Cisco Compliance Solution for PCI are still valid. Nothing in the standard update has affected the guidance provided here.

- **Components:** The solution uses a standardized metric for evaluating a components' native ability to support PCI. This metric is known as the capability scorecard. It summarizes the relevant sections of the PCI DSS for an in-scope device.


Assessment: The capability scorecards of the Cisco Compliance Solution for PCI are still valid. Nothing in the standard update has affected the guidance provided here.

General Changes to the PCI DSS

One of the biggest areas of confusion continues to be the PCI scope definition. The council will provide subsequent guidance in 2015. The PCI 3.0 standard includes wording that clarifies PCI scoping and segmentation to include systems that:

- Provide security services (for example, authentication servers)
- Facilitate segmentation (for example, internal firewalls)
- Affect the security of the cardholder data environment (for example, name resolution or web redirection servers)

¹ The PCI Security Standards Council Participating Organization logo is a trademark or service mark of The PCI Security Standards Council in the United States and in other countries.



The standard also uses the term “isolation” for the first time, as part of the segmentation definition.

The PCI 3.0 standard clarified “out-of-scope systems” to mean those systems that, if compromised, cannot affect the security of the cardholder data environment. Requirement 11.3 has wording that is designed to increase the testing of the cardholder data environment perimeter. It specifies that penetration testing is needed along the internal perimeter, as well as along the external perimeter, to verify that there is no access to sensitive information.

Noteworthy Changes by Requirement

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

- Requirement 1.1.3: Broken out from the network diagram requirement; a new requirement specifically requires maintenance of a data flow diagram that shows all cardholder data flows across systems and networks (effective immediately)
- Requirement 1.1.6: Simple Network Management Protocol (SNMP) versions 1 and 2 added to list of “insecure protocols” (effective immediately)²

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

- Requirement 2.1: Clarified that changing vendor defaults applies to all passwords, including system and application credentials and that unnecessary default accounts are removed or disabled (effective immediately)
- Requirements 2.2.2 and 2.2.3: Make system configuration standards more prescriptive and explicit by breaking out “necessary” services and “secure” services (effective immediately)
- Requirement 2.4: New requirement to maintain current inventory of all PCI system components to develop configuration standards (effective immediately)

Requirement 3: Protect stored data.

No major changes

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.

Requirement 4.1: Bluetooth, CDMA, and satellite communications added to examples of “open public networks” (effective immediately)

Requirement 5: Use and regularly update anti-virus software.

Requirement 5.1.2: Calls for evaluation of evolving malware threats for systems not “commonly affected by malware”

Requirement 6: Develop and maintain secure systems and applications.

- Requirement 6.5.x: New requirement for coding practices to document the way that primary account number (PAN) and sensitive authentication data (SAD) is handled in memory (effective July 1, 2015)
- Requirement 6.5.10: New requirement for coding practices to protect against broken authentication and session management (effective July 1, 2015)

² The Cisco Compliance Solution for PCI already used SNMP version 3 as a baseline in its previous and current versions.

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

No major changes

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

- Requirement 8.3: Clarified that two-factor authentication applies to users, administrators, and all third parties, including vendor access for support and maintenance (effective immediately)
- Requirement 8.5.1: Mandates that service providers must use different credentials to access different customer environments (effective July 1, 2015)

Requirement 9: Restrict physical access to cardholder data.

- Requirement 9.3: New procedures to verify that physical access for terminated employees has been revoked (effective immediately)
- Requirement 9.9.x: New requirement to protect point of sale (PoS) devices that capture payment card data from tampering or unauthorized modification or substitution; requirement includes a list of devices, personnel training, device inspection, etc. (effective July 1, 2015)

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

- Requirement 10.2.x: Enhanced logging requirements, including use of and changes, additions, or deletions to administrative privileges; and stopping or pausing the audit logging system (effective immediately)
- Requirement 10.6.2: Update or clarification stating that logs for all “non-critical” and “non-security” assets must be reviewed “periodically” for malicious activity (effective immediately)

Requirement 11: Regularly test security systems and processes.

- Requirement 11.1.1: New requirement for an inventory of all authorized wireless access points and accompanying business justification (effective immediately)
- Requirement 11.2: Added guidance that multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all vulnerabilities have been addressed (effective immediately)
- Requirement 11.3: Increased specificity for pen test methodology, inclusion of testing segmentation controls, and requirement to retest to validate remediation (effective July 1, 2015)

Requirement 12: Maintain a policy that addresses information security.

- Requirement 12.2.b: New requirement that risk assessments must be performed after significant changes to the environment (effective immediately)
- Requirement 12.8.x: New requirement for maintaining a “responsibilities matrix” that details PCI requirements in scope for service providers (effective immediately)
- Requirement 12.9: New requirement for service providers to acknowledge in writing to the customer that they will maintain all applicable PCI DSS requirements (effective July 1, 2015)

Conclusion

It is the opinion of Cisco and Verizon that 3.0 clarifications impacting technical configurations have been addressed in previous versions of the Cisco Compliance Solution for PCI. The Cisco Compliance Solution for PCI helps you pull everything together to effectively address the PCI Data Security Standard.



For More Information

For more information about the Cisco Compliance Solution for PCI, visit www.cisco.com/go/pci.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)