



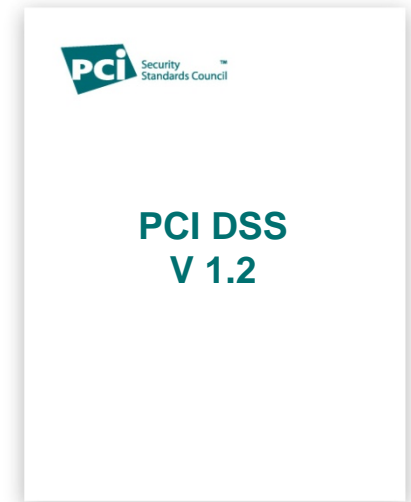
Security
Standards Council

Understanding the PCI DSS Version 1.2

PCI Security Standards Council Webinar Series
November 25 and December 17, 2008

- **Summary of Changes Overview**
- **PCI DSS “Introduction”**
- **The Requirements**
- **Appendices**
- **Q&A**

- Provide greater clarity on PCI DSS requirements
- Offer improved flexibility
- Manage any evolving risks and threats
- Incorporate existing and new best practices
- Clarify scoping and reporting
- Eliminate redundant sub-requirements
- Consolidate documentation



https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf

https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf

- Consolidate PCI DSS documents
 - PCI DSS Requirements and Security Assessment Procedures
- Consistent use of terms throughout
 - “System components,” “cardholder data environment,” “cardholder data”
- Enhance required introductory content for Report on Compliance
- Clarify compensating controls in Appendices B and C
- Add Attestation of Compliance forms
 - Replace current payment brand forms
- Add flowchart for scoping and sampling



Security
Standards Council

PCI DSS “Introduction”

- New PCI DSS v1.2 changes in the “introduction” sections
 - New sections
 - Minor changes to existing sections
- Note that the term “assessor” used in PCI DSS means whoever performs the assessment
 - Whether QSA or Internal Audit staff

- PCI DSS Applicability Information (minor change)
- Scope of Assessment
 - Network Segmentation (new)
 - Wireless (minor change)
 - Third Parties/Outsourcing (minor change)
 - Sampling of Business Facilities and System Components (minor change)
 - Compensating Controls (minor change)
- Instructions and Content for Report on Compliance
 - Report Content and Format (enhanced)
 - Revalidation of Open Items (minor change)
 - PCI DSS Compliance – Completion Steps (new)

- **Scope of Assessment – Network Segmentation**
 - Network segmentation isolates systems that store, process, or transmit cardholder data from those that do not
 - Not a PCI DSS requirement, but can reduce scope, cost, risk
 - Without network segmentation, the entire “flat” network is in scope for PCI DSS
 - Need a clear understanding of business needs that require storage, processing, or transmission of cardholder data
 - Documenting cardholder data flows aids understanding and effective network segmentation
 - No “cook book” approach to network segmentation



Security
Standards Council

The Requirements

- Clarified requirement to illustrate that all sub-requirements apply to both routers and firewalls
- Combined requirements and sub-requirements to clarify requirement 1
- Added flexibility in the time frame for review of firewall rules, from quarterly to every 6 months
 - Based on Participating Organization feedback to allow the control to be customized to the organization's risk management policies



- Clarified wireless requirements in 2.1.1
 - Applies to wireless environments “attached to cardholder environment or transmitting cardholder data”
 - Removed references to WEP
 - To emphasize using strong encryption technologies for wireless networks, for both authentication and encryption
 - Removed requirement to disable SSID broadcast
 - Disabling SSID broadcast does not prevent a malicious user from determining the SSID
 - The SSID is broadcast over numerous other messaging/communication channels



- Clarified use of terms throughout
 - Use “PAN” rather than “data,” “credit card data,” “cardholder data”
 - Use “strong cryptography” and “cryptographic”
 - Refer to Glossary definition of “strong cryptography”
- Clarify 3.4.1
 - Should be “local user account databases”
 - Removable media should be encrypted separately



- Clarified that SSL server must support latest patched versions
- Specified that wireless must be implemented according to industry best practices (e.g., IEEE 802.11i)
 - *New implementations of WEP* not allowed after March 31, 2009
 - *Current implementations* must discontinue use of WEP after June 30, 2010
- Changed “email” in requirement 4.2 to “end user messaging technologies”



- Clarified that anti-virus software applies to all operating system types
 - Remove wording that excluded Unix and mainframes
 - Requirement applies to systems “commonly affected” by malicious software
 - Clarify that where technology exists, anti-virus software must be installed
 - See Navigating PCI DSS document for more information
https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf
- Changed “other malicious software” to “all known types of malicious software”
 - Provide more examples of “malicious software”



- Added flexibility to patching requirement
 - Organization may apply a risk-based approach
- Changed OWASP vulnerabilities to match current OWASP version
- Requirement 6.6 is now mandatory
 - No longer a “best practice”
 - All public-facing web applications are subject to either
 - 1) Reviews of applications via manual or automated vulnerability assessment tools or methods, or
 - 2) Installing an web-application firewall in front of public-facing web applications



- Added separate testing procedures for bullets formerly included at 7.1 and 7.2
 - Clarify tests with further explanation and text
- Clarified user authentication at 8.2 and 8.3
 - Use of password or passphrase
 - Combine token devices and biometrics under “two-factor authentication” and provide examples
 - Explain “remote access”
- Clarified that passwords must be rendered unreadable *in both storage and transmission*
- Clarified tests for database authentication



- Specified that offsite storage locations must be visited at least annually
- Provided flexibility in the requirement for cameras
 - Allow organizations to select other appropriate access control mechanisms
- Changed “periodic” to “at least annually” for visits to offsite storage locations
- Clarified destruction requirements for hardcopy materials and electronic media containing cardholder data
 - Cannot be reconstructed/is unrecoverable
- Clarified that requirement to secure media applies to media that contains cardholder data



- Added “a known, stable version” of NTP “kept current per PCI DSS Requirement 6.1” and eliminated redundant NTP test (10.4.c)
- Clarified that logs for external facing technologies (for example, for wireless, firewalls, DNS and mail) must be copied to an internal log server
- Provided flexibility and clarified that three months of audit trail history must be “immediately available for analysis”
 - Online, archived or restorable from backup



- Changed 11.1 to focus on use of wireless analyzers or wireless IDS/IPS
- Clarified scanning requirements
 - Both internal and external scans required
 - ASVs required to perform quarterly *external* vulnerability scans
 - ASVs not required to perform *internal* scans
- Clarified penetration testing requirements
 - Both internal and external tests required
 - QSAs and ASVs not required to perform tests
 - Web application penetration tests include OWASP



- Expanded list of examples of critical employee-facing technologies
 - Remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and personal digital/data assistants (PDAs)
- Updated timeframe that requires employees to acknowledge that they have read and understood the company's security policy and procedures to “at least annually”
- Combined 12.8 and 12.10
 - Clarified that organizations must have policies and processes to manage and monitor service providers





Security
Standards Council

Appendices

- Appendix A - Clarified hosting providers
 - Applies to shared hosting providers, not all hosting providers
- Appendices B and C - Clarified use and review of compensating controls
- Appendices D and E – New Attestation of Compliance forms
 - Replace current payment brand forms
- Appendix F – New flowchart for scoping and sampling

- Appendix B – Compensating Controls
 - Add and modify four criteria from the Glossary
 - Meet the intent and rigor
 - Provide a similar level of defense
 - Used to say “repel a compromise attempt with similar force”
 - Be “above and beyond”
 - Expanded description with examples
 - Be commensurate with additional risk
- Appendix C – Compensating Controls Worksheet
 - Same content, reformatted to align with SAQs

- Appendix D & E – Attestations of Compliance
 - Attestation forms for merchants (D) and service providers (E),
 - Accepted by all payment brands
 - Completed and signed, and provided to payment brands or acquirers, as applicable
- Appendix F – Scoping and Sampling
 - Flowchart to depict PCI DSS scoping and sampling concepts
 - From Network Segmentation and Sampling of Business Facilities and System Components sections

Want to Understand More?

Check Out “Navigating the PCI DSS v. 1.2 at:

https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf

Questions?

Click on “FAQ” at:

www.pcisecuritystandards.org



Security
Standards Council

Thank you