

SUMMARY

PCI DSS 1.2 — CHANGES AND HOW IT AFFECTS YOUR BUSINESS

Overview

PCI DSS 1.2 is considered a minor update to the current DSS version 1.1. PCI DSS 1.2 has the same 12 requirements as did 1.1 and no new requirements have been added. The intent of 1.2 is mainly to clarify the existing requirements and provide some flexibility in terms of interpretation of the standard.

Important Dates

10/01/2008 – 1.2 Release Date

10/01/2008 – 1.2 Effective Date (All new assessments after this date should use 1.2)

12/31/2008 – 1.1 Sunset Date (All 1.1 assessments should be completed before this date)

03/31/2009 – New WEP implementations are not allowed after this date

06/30/2010 – All WEP implementations must be discontinued as of this date

Changes and New Requirements in PCI DSS 1.2

- Segmentation of network, although not a requirement, the council provided guidance around scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.
- For wireless, the council clarified requirements around use of wireless technology and provided sunset date for use of WEP. Wireless networks should now be implemented using industry best practices like IEEE 801.11X.
- Requirement 6.6 for web application security is now mandatory in 1.2. Additional clarification was provided to remove references to source code review and add use of automated assessment tools.
- Changes in best practices: 1) firewall rule set audit is needed every 6 months (vs. 90 days in 1.1), 2) visit to offsite storage location is required annually and 3) review and acceptance of security policy by employees interacting with cardholder data is required annually.
- Updated the sampling guidelines for assessments and made it more exhaustive across multiple business locations and technologies.
- Announcement of Quality Assurance (QA) program for assessors (QSA, ASV, PA-QSA) to help promote consistency across assessments and provide merchants with good quality assessments.

- Additional documentation in 1.2 include 1) detail documentation of cardholder data environment e.g. list of all tables/files containing cardholder data and 2) compensating controls should be documented, reviewed and validated by an assessor annually.

Future Improvements for PCI DSS

- PCI 1.2 is still largely focused on securing the perimeter to stop bad guys from getting in. There is a desire in the security community to see more requirements around addressing internal threats.
- The current DSS only addresses requirements around storage of cardholder data after authorization, but is still largely silent about storage of data before authorization.
- New challenges like virtualization will need to be addressed in the near future as well.

PCI DSS 1.2 Changes to the 12 Requirements

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- Now talks about firewall as well as router configurations.
- Review configuration and rule sets every 6 months instead of every quarter.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- Wireless requirements apply only to networks touching cardholder data.
- Remove mention of WEP.

Requirement 3: Protect Stored Cardholder Data

- If disk encryption is used, make sure it's separate from the OS encryption.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- Wireless networks should now be implemented using industry best practices like IEEE 801.11X.
- New WEP implementations not allowed after March 31, 2009. Ideally should not be implemented anymore.
- All WEP implementations must be discontinued as of June 30, 2010.
- Disallow sending unencrypted PAN info in all end-user messaging systems like IM, chat and SMS and not just in e-mails.

Requirement 5: Use and Regularly Update Anti-Virus Software

- Expand definition of antivirus to include all known types of malware like Trojans, worms, rootkits, etc.

Requirement 6: Develop and Maintain Secure Systems and Applications

- Patching can now be risk based instead of fixed 30 days for all systems in scope.
- Organization can identify highest risk systems and patch those in 30 days and then focus on patching of lower risk systems.
- All custom code must be developed as per latest OWASP guidelines at time of development.
- Incorporate source code review as part of regular software development life cycle (SDLC). The code can be reviewed by trained, independent internal team or specialized external tools/organizations.
- Source code review removed from requirement 6.6. For ongoing protection of public facing web applications, either of the following can be used:
 1. Regular use of automated or manual application vulnerability assessment tools or methods. (can be performed by trained, independent internal team or specialized external tools/organizations)
 2. Properly configured web application firewall with capabilities in line with the special 6.6 information supplement released by the council.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

- No major changes.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

- Testing must verify that passwords are unreadable in both storage and transmission.

Requirement 9: Restrict physical Access to Cardholder Data

- Visit in-scope offsite storage facility at least once per year.
- Removable electronic media as well as paper media (fax, printouts, etc.) must be secured.
- Cameras need to be used only for storage facilities and datacenters and not POS locations.
- For purpose of PCI, a contractor is treated same as employee and same access requirements apply.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

- Must copy logs from external facing devices to a secure internal location.
- Minimum 3 months of logs must be immediately available (within reasonable time) for analysis.

Requirement 11: Regularly Test Security Systems and Processes

- Wireless IDS/IPS can be used as an option to wireless analyzer as long as it is correctly setup to alert someone when there is an incident.
- Approved Scanning Vendor (ASV) must be used to perform quarterly external network vulnerability scans.
- Penetration testing must occur on external as well as internal devices. ASV not required for penetration test.

Requirement 12: Maintain a Policy That Addresses Information Security

- Develop usage policies for employee-facing technologies including everything from USB drives to PDA and iPhone.
- Employees interacting with cardholder data must read and acknowledge security policies at least once a year.
- Clarify language around relationship with service providers and maintain written agreement with service provider detailing their responsibilities around cardholder data.
- Changes in this requirement also seems to suggest that merchant's PCI compliance is not held up if service provider is not PCI compliant as long as the service provider is in the process of becoming PCI compliant and the merchant monitors the progress on an ongoing basis.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys Hong Kong Ltd. • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 2824 8488

