PCI DSS v4.0 AT A GLANCE

MAJOR DIFFERENCES BETWEEN V4.0 AND V3.2.1

online

1

NETWORK SECURITY

Simpler. Clearer. Applies to all methods of connectivity and segmentation controls. Even CDE wireless must be segmented from the rest of the CDE.

2

SYSTEM HARDENING

Added recognition that one-function per server allows difficult to separate services, like Active Directory and DNS, to live on single systems with appropriate protections.

3

PROTECT ACCOUNT DATA AT REST

Protect SAD at rest, just like CHD, even if storage is temporary. Prevent copying, local storage, and other easy exfiltration of CHD. Use full disk and volume encryption for removable media only.

4

PROTECT CARDHOLDER DATA IN TRANSIT

Inventory and track the keys and certificates used to secure account data in transit. This includes self-signed certificates, if used.

5

ANTI-MALWARE

Next-gen and behavior based anti-malware officially acceptable. Periodic evaluations of systems not known to be affected by malware, as opposed to commonly affected, still required. Processes and automated mechanisms must be in place to protect against phishing attacks.

6

MANAGE VULNERABILITIES, CHANGES, AND SOFTWARE DEVELOPMENT

More relevant, comprehensive development security. Inventory software dependencies, track and handle their vulnerabilities. Protect against web-skimming and use automated web app protections.

7

AUTHORIZATION

Extended the DSS-required role-based and least privilege access model to application and system accounts.

8

AUTHENTICATION AND PASSWORD SECURITY

Strictly control and track any interactive and needed use of shared, application, and service accounts. 12-character passwords and risk-based expiration. Ensure even admins cannot bypass MFA, which is required for remote access AND for CDE access by users in any role (yes, maybe twice).

9

FACILITIES, MEDIA, AND POI DEVICE SECURITY

Streamlined with better grouping of physical access, visitor access, media handling, and POI requirements. POI device inspection frequency based on targeted risk assessment.

10

LOGGING AND MONITORING

Automate security log reviews. Monitoring for, responding to, and correcting control failures will apply to everyone after 31 March 2025.

11

VALIDATION AND TESTING

Implement authenticated internal vulnerability scanning. Correct all vulnerabilities, including medium and low severity. More anti-web-skimming: client-side payment page integrity checking.

12

SECURITY AND COMPLIANCE PROGRAM

Perform targeted risk assessments for control frequencies and customized approaches. Assess cryptography and outdated systems risks. Routinely verify PCI scope. Specific IRPs for PAN data discovered outside the CDE.

GENERAL CHANGES

Entire DSS re-ordered to emphasize accountability. Terms [re]defined to clarify protections apply to all account data, frequencies of activity, and what constitutes a significant change. Customized approaches to meeting requirement objectives supported.

A1

MULTI-TENANT SERVICE PROVIDERS

Applies to all cloud-, hosting-, payment-, and other-service providers. Employ segregation to ensure customer tenants cannot access or interfere with each other. Accept and handle incident reports from tenant customers.

A2

CARD-PRESENT POI DEVICES USING SSL/EARLY TLS

Only applies and allows use of some older POI devices. Not eligible for a customized approach.

A3

DESV

Not eligible for a customized approach. Scoping requirements aligned with and incorporated into Requirement 12.

Results. Guaranteed.