PCI DSS 4.0.1 Update

March 2025

On 31 March 2025, new requirements under the PCI DSS version 4.0.1 standard will become mandatory.

As a result, the criteria for a compliant Self-Assessment Questionnaire (SAQ) will change. This will affect SAQs that have been partially completed or not yet started. Any SAQ that has not been completed by 31 March must be reset and completed as an updated version. SAQs finalized before this date will remain valid until annual recertification.

To expedite your SAQ processing, and stay compliant and secure, consult your VENZA Security Analyst to complete any pending SAQs by this date.

Updated Requirements

Below is a summary of notable updates impacting the PCI DSS assessment process with the transition to version 4.0.

For a detailed overview of all new and updated requirements introduced in PCI DSS version 4.0.1, click here.

1. Disk-Level Encryption Changes (Requirement 3.5.1.2)

- Disk-level encryption will no longer be sufficient for protecting stored data, except for removable electronic media.
- Organisations must adopt more granular encryption methods, such as:
    - File-level encryption.
    - Column-level encryption for databases.
    - Data-level encryption before storage.

2. Secure Transmission of Cardholder Data (Requirement 4.2.1)

- To ensure security and prevent exploitation, certificates used to send Primary Account Numbers (PAN) over open or public networks must be:
    - Valid.

    - Not expired or revoked.

3. Malware Risk Assessments (Requirement 5.2.3.1)

- All systems in scope must be regularly checked for malware vulnerabilities.
- This process should include:
    - Clear procedures for determining which systems are susceptible to malware.
    - Implement controls to protect those systems.

4. Removable Media Scans (Requirement 5.3.3)

- To mitigate the risks posed by external devices, removable media (e.g., USB drives) must be scanned and continuously monitored for malware.

5. Phishing Protection (Requirement 5.4.1)

- As phishing remains a leading attack vector, organisations must implement processes and automated tools to combat it. Examples of required tools include:
    - Email filtering.
    - Link analysis tools (link scrubbers).

6. Web Application Security (Requirement 6.4.2)

- Manual reviews will no longer be sufficient to protect public-facing web applications.
- Instead, ongoing automated monitoring and protection must be implemented using a technical solution, such as a Web Application Firewall (WAF), to defend against web-based attacks.

7. Payment Page Script Management (Requirement 6.4.3)

- To address the risk of malicious script injections, organisations must manage and verify payment page scripts to ensure authorization and integrity.

8. Automated Change Detection (Requirement 11.6.1)

- Organisations must deploy automated tools to monitor and detect changes to critical files, including:
    - Operating system files.
    - Application files.
    - Configuration files
- Any unauthorized changes must trigger an alert, be logged, and reviewed to quickly respond to potential security threats.

9. User and System Account Reviews (Requirements 7.2.4 & 7.2.5)

- To ensure that both user and system access are controlled and monitored:

    - User accounts must be reviewed at least every six months.
    - Application and system accounts must be periodically reviewed.

10. Authenticated Internal Vulnerability Scans (Requirement 11.3.1.2)

- Internal vulnerability scans must be conducted using credentials from a privileged access account to ensure thorough identification of vulnerabilities.

11. Addressing All Vulnerabilities (Requirement 11.3.1.1)

- All identified vulnerabilities, including low and medium risks, must be addressed based on the organisation's targeted risk analysis.
- Even low- or medium-risk vulnerabilities must be assessed and mitigated appropriately; they cannot be ignored.

12. Cryptographic Standards Review (Requirement 12.3.3)

- To maintain strong encryption amidst evolving cryptographic standards, organisations must:
    - Formally review cryptographic suites and protocols annually.
    - Continuously monitor industry trends to ensure encryption mechanisms remain current, effective, and secure.

13. Technology Effectiveness Review (Requirement 12.3.4)

- All hardware and software must be formally reviewed annually to ensure:
    - They remain effective.
    - They have not reached end-of-life status.

14. Incident Response for Sensitive Data (Requirement 12.10.7)

- To ensure rapid response and containment of incidents involving sensitive cardholder data:
    - Incident response plans must address incidents where Primary Account Numbers (PAN) are found outside of authorized locations.
    - This includes providing clear steps for containing and addressing potential data breaches.

About VENZA

VENZA is the leading provider of cybersecurity, data protection, and compliance solutions for the hospitality industry. Drawing on decades of experience, VENZA provides 360-degree visibility that enables proactive risk management to mitigate vulnerabilities and keep your guests and their data safe. Know your risks and protect your enterprise with VENZA.

Visit www.VENZAGroup.com for additional details.

Contact Us

Sales: sales@venzagroup.com

Security Team: securityanalyst@venzagroup.com