

How should PCI DSS v4.x requirements noted as superseded by another requirement be reported after 31 March 2025?

PCI SSC FAQ | Article 1593 | March 2025

After 31 March 2025, superseded requirements should be marked as Not Applicable (N/A) in a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ).

Three PCI DSS v4.x requirements include a note that the requirement will be superseded by another requirement as of 31 March 2025.

The table below shows the three requirements, with the effective requirement and superseded requirement noted in each case.

Requirement Number and Description *

Effective as of

31 March 2025

Superseded – N/A after 31 March 2025

6.4.2 - For public-facing web applications, deploy an automated technical solution to detect and prevent web-based attacks.

X

6.4.1 - Review public-facing web application via manual or automated application vulnerability security assessment tools/methods or deploy an automated technical solution to detect and prevent web-based attacks.

X

8.3.10.1 - If passwords/passphrases are used as the only authentication factor for customer user access, service providers change customer passwords at least once every 90 days or determine access to resources based on dynamic analysis of accounts' security posture.

X

8.3.10 - If passwords/passphrases are used as the only authentication factor for customer user access, service providers provide guidance to customers about frequency, when, and under which circumstances to change passwords/passphrases.

X

10.7.2 - Failures of critical control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical control systems:

· <10 bullets>

X

10.7.1 - Failures of critical control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical control systems:

· <8 bullets>

X

* Refer to PCI DSS v4.x for the exact wording of the requirement.

Source: <https://www.pcisecuritystandards.org/faqs/1593/>