

Can entities be PCI DSS compliant if they have performed vulnerability scans at least once every three months, but do not have four "passing" scans?

PCI SSC FAQ | Article 1152 | January 2024

PCI DSS requires entities to perform internal and external vulnerability scans at least once every three months, identify and address vulnerabilities in a timely manner, and verify through rescans that vulnerabilities have been addressed. To achieve these objectives, an entity would need to show that "clean" or "passing" scans were performed at least once every three months for the previous four quarters, for both their external and internal environments. A "clean" or "passing" scan generally has the following characteristics:

- No configuration or software was detected that results in an automatic failure (such as the presence of default accounts and passwords, etc.)
- For external scans, no vulnerabilities with a score of 4.0 or higher on the Common Vulnerability Scoring System (CVSS)
- For internal scans, vulnerabilities are resolved by the entity according to PCI DSS Requirement 11.3.1.

With new vulnerabilities continually being identified, scanning becomes an integral part of an organization's vulnerability management process, resulting in a cycle of scanning, patching, and rescanning until a "clean" scan is obtained. However, due to the frequency of new vulnerabilities being identified, it may not always be possible to produce a single, clean scan at least once every three months. Take the example of an entity that performs a scan which identifies several vulnerabilities. The entity then fixes all the identified vulnerabilities and performs a rescan to verify. The rescan shows that the vulnerabilities identified in the first scan have been addressed, but new vulnerabilities that were not present in the original scan have since appeared. In this case, instead of having a single, environment-wide scan report, an entity may verify they have met the scanning requirements through a collection of scan results which together show that all required scans are being performed, and that all applicable vulnerabilities are being identified and addressed at least once every three months.

To verify that the requirement to perform vulnerability scans at least once every three months has been met, the following should occur:

- Scans of all in-scope systems are performed at least once every three months, and all in-scope systems are covered by the entity's scan-remediate-rescan processes.
- Rescans are performed as necessary and show that vulnerabilities identified in the initial scans have been remediated, for all affected systems, as part of that period's scanning process.
- The entity has processes in place to remediate currently identified vulnerabilities.
- Repeated failing scans are not the result of poor remediation practices resulting in

previously identified vulnerabilities not being properly addressed.

If, however, an entity does not have four passing scans for the last 12 months, performed at least once every three months, because they didn't schedule the scans properly, or the scans are incomplete, or the identified vulnerabilities have not been addressed from one period to the next, then the entity has not met the requirement.

Note: results from external vulnerability scans may also be required by acquirers and payment card brands as part of an entity's annual compliance validation. Entities should contact their acquirer (merchant bank) and/or the payment brands directly to understand their reporting requirements for external scans.

Source: <https://www.pcisecuritystandards.org/faqs/1152/>