

For vulnerability scans, what is meant by "quarterly" or "at least once every three months"?

PCI SSC FAQ | Article 1087 | July 2023

The intent of conducting vulnerability scans "quarterly" or "at least once every three months," as defined in PCI DSS v3.2.1 and v4.0 respectively, is to have them conducted as close to three months apart as possible, to ensure vulnerabilities are identified and addressed in a timely manner. To meet the vulnerability scanning requirements in PCI DSS Requirement 11, an entity is required to complete their internal and external scans, and perform any required remediation, at least once every three months.

At least once every three months, or 90 days, is considered the maximum amount of time that should be allowed to pass between quarterly vulnerability scans. If unforeseen circumstances occur that impact an entity's ability to complete scheduled scans, every effort should be made to perform scans as soon as possible (for example, within a day or two) of the scheduled scan date. Where an entity has advance notice of factors that may delay scans or impede their ability to address vulnerabilities (for example, scheduled system downtime, or predefined no-change windows that prevent system updates), the entity should strive to schedule scans before the three-month period is reached.

Entities are encouraged to perform vulnerability scans more frequently than required as it will enhance security by allowing quicker identification and resolution of vulnerabilities. More frequent vulnerability scans also provide entities with earlier awareness of vulnerabilities that need to be resolved, thereby increasing the likelihood that all vulnerabilities are successfully identified and resolved within the three-month period.

PCI DSS also requires vulnerability scans after significant changes. These scans are required in addition to the scans conducted at least once every three months; this means that vulnerability scans are required both 1) at least once every three months and 2) after a significant change.

Also refer to the following related FAQ:

-

FAQ 1572: Can a compensating control be used for requirements with a periodic or defined frequency, where an entity did not perform the activity within the required timeframe?

Source: <https://www.pcisecuritystandards.org/faqs/1087/>