

What are the expectations for entities when assigning risk rankings to vulnerabilities and resolving or addressing those vulnerabilities?

PCI SSC FAQ | Article 1597 | May 2025

There are several PCI DSS requirements that govern vulnerability management and reference related timeframes. These requirements are described under the general topics of 1) identifying and risk ranking vulnerabilities, and 2) resolving or addressing vulnerabilities.

Vulnerability Management Infographic
(<https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Vulnerability%20Management%20Infographic.pdf>)

Identify and risk-rank vulnerabilities:

Requirements 11.3.1 and 11.3.1.1 specify internal vulnerability scans. The information from an entity's internal vulnerability scans should be used as one of the inputs into the entity's processes for identifying and risk-ranking vulnerabilities at Requirement 6.3.1.

After finding the vulnerabilities, Requirement 6.3.1 specifies that entities manage security vulnerabilities, including assigning risk rankings based on impact to the entity and identifying at a minimum those vulnerabilities considered to be high-risk or critical to the entity's environment. Note that Requirement 6.3.1 does not require that an entity accepts risk rankings assigned by external sources; rather the entity may evaluate external risk rankings considering the entity's risk and environment and then assign the appropriate risk ranking for the entity's environment.

Resolve or address vulnerabilities:

Requirements 11.3.1 and 11.3.1.1 also specify that critical and high-risk vulnerabilities are resolved*, and that lower-ranked vulnerabilities are addressed** in accordance with the entity's risk as defined and documented in a targeted risk analysis (TRA).

PCI DSS Requirement 6.3.3 specifies time frames for installing security patches/updates – those for critical vulnerabilities must be resolved within one month of release. Additionally, all other applicable security patches/updates must be installed within appropriate time frames determined by the entity's assessment of the risk to their environment. The appropriate time frames defined by the entity should align with the risk ranking of vulnerabilities assigned in Requirement 6.3.1 (for example, resolving high-risk vulnerabilities more quickly than lower-ranked vulnerabilities). Refer to the Requirement 6.3.3 Guidance column under Examples for more information.

* Resolved – the entity solves or fixes the vulnerability.

** Addressed – the entity determines whether to resolve the vulnerability or to mitigate the risk by addressing the vulnerability in another way (e.g., with a

compensating control or by disabling a vulnerable service).

Source: <https://www.pcisecuritystandards.org/faqs/1597/>