

How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date?

PCI SSC FAQ | Article 1564 | March 2023

Where a future-dated requirement has not yet been implemented by an entity and the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) is completed prior to the effective date of the new requirement, the future-dated requirement can be marked as "Not Applicable."

Where an entity relies on a third-party service provider (TPSP) to meet PCI DSS requirements on the entity's behalf, and:

-

The TPSP has not yet been assessed against the new version of the standard,

Or

-

The TPSP has been assessed to the new version of the standard, but the assessment was prior to the effective date of new requirements that the TPSP is meeting on the entity's behalf, and did not include those new requirements,

Then, providing that the TPSP has a current PCI DSS assessment (within the last 12 months) against a version that was current at the time of the assessment, the entity's assessor may mark those requirements upon which the entity relies as "Not Applicable."

If an entity or TPSP has implemented a future-dated requirement prior to its effective date and wants to include it in its PCI DSS assessment, they may choose to do so.

In all cases, commencing on the effective date of new PCI DSS requirements, all new requirements applicable to an entity's assessment (including those met by a TPSP on the entity's behalf) must be fully considered as part of the entity's PCI DSS assessment.

Also refer to the following related FAQs:

-

FAQ 1563: What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-an-entity-do-if-its-pci-dss-assessment-will-not-be-complete-prior-to-that-standard-s-retirement-date/)

-

FAQ 1328: Where can I find the current version of PCI DSS? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/where-can-i-find-the-current-version-of-pci-dss/)

-

FAQ 1565: Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired?

-

FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released — should the assessment be started again using the new version?

Source: <https://www.pcisecuritystandards.org/faqs/1564/>