

# Can a partial PCI DSS assessment be documented in a Report on Compliance (ROC)?

PCI SSC FAQ | Article 1382 | August 2024

---

Yes. Where an entity wants its assessor to conduct a PCI DSS assessment against only a subset of PCI DSS requirements, it is acceptable to document this partial assessment using the Report on Compliance (ROC). The Attestation of Compliance (AOC) is also completed after a PCI DSS assessment to summarize and attest to the results of the assessment.

There are a number of reasons why an entity may want to undergo a partial assessment, including:

- An entity only needs to validate a subset of requirements to their acquirer (for example, using the prioritized approach to validate only certain milestones);
- An entity wants to validate a new security control that impacts only a subset of requirements (for example, a new encryption methodology requiring assessment to PCI DSS Requirements 3 and 4);
- A service provider identifies which PCI DSS requirements are included in the scope of their service offering and only wants those covered in the assessment (for example, a data center hosting provider only wants to validate physical security controls per PCI DSS Requirement 9 for their hosting facility);
- During a Token Service Provider (TSP) engagement, the TSP assessor determines that a partial PCI DSS assessment will adequately address the additional considerations for PCI DSS Requirements 1-12 that affect TSPs.

When documenting such an assessment, the assessor is expected to clearly communicate that testing of all requirements has not been performed by documenting which specific requirements were tested and which were not tested within both the ROC and the AOC.

The PCI DSS ROC Template provides detailed instructions on how to properly define the scope of the assessment, and how to properly document the findings from the testing performed, including the difference between "Not Tested" and "Not Applicable" responses. Accurate documentation of assessment activities performed and related findings provides readers of the report a clear understanding of the report and removes any ambiguity about the scope of the assessment review.

Note that whether a "Not Tested" response can result in PCI DSS compliance is treated differently between PCI DSS v3.2.1 and v4.0 - QSAs must refer to the ROC Template and ROC Template FAQs for the version of the standard being used for relevant guidance.

See also:

FAQ 1473: What is the role of compliance-accepting entities and assessors in determining the applicability of PCI DSS requirements for merchant and service provider PCI DSS assessments?

([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/What-is-the-role-of-compliance-accepting-entities-and-assessors-in-determining-the-applicability-of-PCI-DSS-requirements-for-merchant-and-service-provider-PCI-DSS-assessments](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-is-the-role-of-compliance-accepting-entities-and-assessors-in-determining-the-applicability-of-PCI-DSS-requirements-for-merchant-and-service-provider-PCI-DSS-assessments))

FAQ 1331: Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments in a Report on Compliance? ([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/can-saq-eligibility-criteria-be-used-as-a-guide-for-determining-applicability-of-pci-dss-requirements-for-merchant-assessments-documented-in-a-report-on-compliance/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-saq-eligibility-criteria-be-used-as-a-guide-for-determining-applicability-of-pci-dss-requirements-for-merchant-assessments-documented-in-a-report-on-compliance/))

Source: <https://www.pcisecuritystandards.org/faqs/1382/>