

# 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?

PCI SSC FAQ | Article 1473 | March 2023

---

Compliance-accepting entities (typically, payment brands and acquirers) are responsible for determining the PCI DSS validation and reporting methods of their merchants and service providers, including how compliance is to be evidenced—for example, whether via a Report on Compliance (ROC) or a Self-Assessment Questionnaire (SAQ). Compliance-accepting entities may also provide direction to their customers about which PCI DSS requirements to include in the assessment—for example, they may require that only a specific subset of PCI DSS requirements, such as those included in an SAQ, be tested and the results documented in a ROC.

Assessors are responsible for validating that the scope of the assessment and that applicability of PCI DSS requirements is accurately defined and documented. To report a PCI DSS requirement as 'Not Applicable', the assessor must first confirm through testing that the requirement is truly not applicable to that environment. This confirmation must be performed and documented for all "Not Applicable" responses before a compliant result can be considered for the assessment.

Alternatively, a "Not Tested" response is used for assessments where a requirement (or a single aspect of a requirement) is not tested in any way – this means the requirement (or aspect thereof) is completely excluded from the assessment without any consideration as to whether it does or could apply.

If a compliance-accepting entity directs an assessed entity or its assessor to exclude any PCI DSS requirement(s) from an assessment, that requirement(s) must be marked as 'Not Tested.'

The PCI DSS ROC Template provides detailed instructions on how to properly document the findings from the testing performed, including the difference between "Not Tested" and "Not Applicable" responses.

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 the ROC Template FAQs for the version of the standard being used for relevant guidance.

Entities should contact the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in [FAQ 1142: How do I contact the payment card brands?](#)

See also:

[FAQ 1382: Can a partial PCI DSS assessment be documented in a Report on Compliance \(ROC\)?](#)

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/1473/>