

Can a Qualified Security Assessor (QSA) rely on the results from non PCI DSS assessment (for example, a SOC 2 or SOC 3 audit) for a PCI DSS assessment?

PCI SSC FAQ | Article 1567 | March 2023

No, due to the variability of scope coverage and assessor validation procedures, a QSA cannot rely on reports from other attestation engagements (like SOC 2 or SOC 3) for a PCI DSS assessment. However, a QSA may be able to use the evidence generated during those assessments for a PCI DSS assessment, but only after independently reviewing the evidence and gaining assurance that:

-

The scope of the assessment includes the relevant payment environment(s) and payment account data,

-

What was covered directly maps to PCI DSS requirements,

-

The evidence is within the timeframe of the PCI DSS assessment and meets any specifics called out in related PCI DSS testing procedures, and

-

That relevant PCI DSS controls are "in place."

See also FAQ 1566: Can a Qualified Security Assessor (QSA) ask an auditor from the same company (for example, one conducting a SOC 2 or SOC 3 audit) to collect evidence for a PCI DSS assessment? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-a-qualified-security-assessor-qa-ask-an-auditor-from-the-same-company-for-example-one-conducting-a-soc-2-or-soc-3-audit-to-collect-evidence-for-a-pci-dss-assessment/)

Source: <https://www.pcisecuritystandards.org/faqs/1567/>