

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?

PCI SSC FAQ | Article 1566 | March 2023

Yes. However, regardless of how the QSA obtains evidence to support a PCI DSS assessment, the QSA conducting the PCI DSS assessment has the ultimate responsibility for their client's assessment and the accuracy and relevance of the information and evidence provided in the Report on Compliance and related workpapers.

This responsibility includes that the QSA evaluates the evidence and confirms that:

- Collected evidence is specific to the scope of the PCI DSS assessment,
- Collected evidence directly relates to the specific PCI DSS requirement under review,
- The date of the evidence is within the scope of the assessment and meets any specifics called out in related PCI DSS testing procedures, and
-

The QSA can effectively render an opinion based on the collected evidence about whether the relevant controls are "in place."

See also FAQ 1567: 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?

Source: <https://www.pcisecuritystandards.org/faqs/1566/>