

How should QSA assistance with completion of Self-Assessment Questionnaire (SAQs) be documented?

PCI SSC FAQ | Article 1445 | February 2017

PCI SSC does not define specific reporting requirements for QSAs assisting merchants with Self-Assessment Questionnaires (SAQs).

Before beginning any engagement, the QSA should have a clear understanding of their expected role for the engagement. If the QSA's client is requesting assistance with their self-assessment, the type and level of assistance should be clearly defined and understood by both parties. Similarly, if a merchant's acquirer stipulates that a QSA must be involved in the merchant's self-assessment, the QSA and merchant should confirm with the acquirer what activities the QSA is expected to perform, including the level of testing and documentation, as applicable. For example, the QSA may be requested to provide guidance to help the merchant determine their PCI DSS scope, or assist with interpretation of PCI DSS requirements, or perform testing to validate that controls were in place. It is important that responsibilities are clearly defined for all parties — including the acquirer, merchant, and QSA — and that each party understands their responsibilities in the process.

In all instances, the QSA should clearly document the role they performed in the QSA Acknowledgement section (Part 3c) in the applicable SAQ. Similarly, Part 3d of the SAQ provides the ability for an ISA to document their involvement, if applicable, in the assessment.

Source: <https://www.pcisecuritystandards.org/faqs/1445/>