

What are the Council's requirements for QSA and ASV Companies to maintain a Quality Assurance (QA) manual?

PCI SSC FAQ | Article 1169 | October 2012

Companies participating in a PCI SSC program, including QSAs and ASVs, must establish and maintain an internal quality assurance (QA) process as set forth by the individual program's qualification or validation requirements. These QA processes must also be formally documented within an internal QA manual. The Council recognizes that each organization has unique needs and therefore does not mandate specific requirements to be included within an organization's QA manual; however, the following items have been identified as a set of best practices which are expected to be present:

- Company name
- List of PCI SSC programs the company participates in
- Descriptions of job functions or responsibilities
- Identification of QA manual process owner
- Approval and sign-off processes
- Requirements for independent quality review of work product
- Requirements for handling and retention of work papers
- QA process flow
- Distribution and availability of the QA manual
- Evidence of annual review by the QA manual process owner

The QA manual should cover all activities relevant to the particular program. QSAs and ASVs should refer to their respective Validation Requirements and Program Guides for information concerning program-specific requirements.

Source: <https://www.pcisecuritystandards.org/faqs/1169/>