

What are the steps needed to perform a self assessment to validate compliance with PCI DSS?

PCI SSC FAQ | Article 1134 | July 2015

Merchants and service providers that validate PCI DSS compliance using a Self-Assessment Questionnaire (SAQ) will typically complete the following steps:

-

Identify the SAQ that applies to your environment, using the Self- Assessment Questionnaire Instructions and Guidelines document (available in the PCI SSC Documents Library) for guidance. Merchants should consult with their acquirer (merchant bank) or the payment brands directly to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

-

Confirm your environment is properly scoped and meets all the eligibility criteria for the SAQ being used.

-

Perform the self-assessment activities as described in the Expected Testing column of the SAQ, and enter a response for each requirement included in the SAQ.

-

Complete all sections of the SAQ and Attestation of Compliance (AOC). AOCs are included within each SAQ and also provided as separate, standalone documents.

-

If required as part of your compliance, complete external vulnerability scans using a PCI SSC Approved Scanning Vendor (ASV), and obtain passing scan reports from the ASV.

-

Submit the required documentation to your acquirer or payment brand, in accordance with the applicable payment brand compliance programs. Your compliance documentation may include the full SAQ, AOC, and/or ASV scan reports, as well as other documentation requested by your acquirer or payment brand.

Source: <https://www.pcisecuritystandards.org/faqs/1134/>