

Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments documented in a Report on Compliance?

PCI SSC FAQ | Article 1331 | May 2025

Service providers cannot use SAQ eligibility criteria to determine applicability of PCI DSS requirements for assessments documented in a Report on Compliance (ROC). The only acceptable SAQ for service providers is SAQ D for Service Providers. All other SAQs are intended for merchant use only.

Merchants should work with their QSA to fully understand the merchant's environment. If they are able to reach agreement that applying only the requirements included in an SAQ is an acceptable approach to secure that merchant's environment, then that SAQ may be used as a relevant guide for applicability of PCI DSS requirements for that environment. If an environment meets some but not all eligibility criteria for a particular SAQ, then the SAQ should not be considered a relevant guide for applicability of requirements. This approach must be clearly documented by the QSA in "Description of Scope of Work and Approach Taken" section 3.1 of the (ROC).

The assessor will need to perform appropriate testing and validation to verify the non-applicability of any PCI DSS requirements. As an example: If an e-commerce merchant has a webserver using a server-side redirect (for example, HTTP response with a status code 301 or 302) to a PCI DSS compliant third-party payment processor, the assessor could consider requirement 6.4.3 and 11.6.1 as not applicable since the redirection mechanism is not susceptible to script-based attacks.

This approach must be clearly documented by the QSA in "Description of Scope of Work and Approach Taken" section 3.1 of the ROC. Any PCI DSS requirements verified by the assessor to be not applicable should be reported as "Not Applicable" in accordance with instructions in the ROC Template. Assessors should refer to the ROC Template and ROC Template FAQs for the version of the standard being used for relevant guidance.

In all cases, the merchant is still expected to include PCI DSS Requirement 12.5.2 to document and confirm their PCI DSS scope at least once every 12 months. The merchant's assessor is expected to include an assessment of Requirement 12.5.2 and document results in the merchant's ROC. See PCI DSS v4.x "Annual PCI DSS Scope Confirmation" for more details.

Merchants should always consult with the organizations that manage compliance programs (for example, payment brands and acquirers) to confirm their PCI DSS validation and reporting method. If a detailed assessment and ROC is the appropriate method, merchants meeting the eligibility criteria from an SAQ should also confirm that the approach outlined above is acceptable. Contact information for the payment

brands can be found in FAQ #1142 How do I contact the payment card brands?
([https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-d
o-I-contact-the-payment-card-brands](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands))

Source: <https://www.pcisecuritystandards.org/faqs/1331/>