

Can service providers use eligibility criteria from a merchant Self-Assessment Questionnaire (SAQ) to determine applicable PCI DSS requirements for the service provider's assessment?

PCI SSC FAQ | Article 1578 | June 2024

No. It was never the intent that a service provider uses a merchant SAQ to determine applicable requirements for a service provider's PCI DSS assessment. The only correct SAQ for a service provider is SAQ D for Service Providers. All other SAQs are intended only for merchants.

Certain merchant SAQs include a reduced set of applicable requirements because, to be eligible for that SAQ, the merchant must have outsourced all storage, processing, and transmission of account data to a PCI DSS compliant service provider. Many requirements with important security controls are not included in those SAQs specifically because it is expected that the service providers used by these merchants are meeting those PCI DSS requirements on the merchant's behalf. A service provider that only meets the reduced set of requirements in these SAQs will be missing these important security controls. In addition, there are numerous requirements noted as "Additional requirement for service providers only" in SAQ D for Service Providers - these requirements are not included in any merchant SAQ.

All PCI DSS requirements must be considered when scoping a service provider's assessment to determine which requirements are applicable to the service being provided and the systems providing that service. To the extent that a given service provider offers a limited service for merchants, for example one that only indirectly facilitates storage, processing, or transmission of payment data, those service providers are still expected to comply with all applicable PCI DSS requirements related to the service and the systems that provide that service.

If a given PCI DSS requirement is truly not applicable to a service provider (for example, the software development ones in Requirement 6 because the service provider does not develop software), those requirements can be marked as N/A.

A service provider that provides a merchant SAQ or a merchant Attestation of Compliance (AOC) as evidence of its PCI DSS compliance has not provided sufficient evidence for its customers.

Source: <https://www.pcisecuritystandards.org/faqs/1578/>