

# What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance?

PCI SSC FAQ | Article 1576 | February 2024

---

If the TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer, and that the relevant PCI DSS requirements were examined and determined to be in place. If the TPSP has a PCI DSS Attestation of Compliance (AOC), it is expected to provide the AOC to customers upon request. This AOC should be applicable to the services the TPSP provides to the customer(s) and provide evidence that the PCI DSS requirements relevant to those services are met. The customer may also request relevant sections of the TPSP's PCI DSS Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) D for Service Providers.

If the TPSP does not undergo its own PCI DSS assessment and or otherwise does not have an applicable AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that the customer (or its assessor) is able to confirm that the TPSP is meeting those PCI DSS requirements.

In addition, in accordance with PCI DSS Requirement 12.9.1 and 12.9.2, the TPSP is obligated to provide information to its customers about which PCI DSS requirements for which the TPSP is responsible, and which are the responsibility of the customer. One tool that can be used to document and share this information is a responsibility matrix, a sample of which can be found in Appendix B of the Information Supplement: Third-Party Security Assurance ([https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/ThirdPartySecurityAssurance\\_March2016\\_FINAL.pdf](https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/ThirdPartySecurityAssurance_March2016_FINAL.pdf)) on the PCI SSC website.

For more information, refer to the PCI DSS section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers.

Refer to the following FAQs:

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? ([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/))

FAQ 1354: Can sensitive information be redacted from the PCI DSS Attestation of Compliance before it is shared with other entities? ([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/Can-sensitive-information-be-redacted-from-the-PCI-DSS-Attestation-of-Compliance-before-it-is-shared-with-other-entities/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/Can-sensitive-information-be-redacted-from-the-PCI-DSS-Attestation-of-Compliance-before-it-is-shared-with-other-entities/))

FAQ 1290: If an entity uses a third-party service provider (TPSP) that has been validated as PCI DSS compliant, is the entity's assessor required to go onsite to the TPSP's location and retest the PCI DSS requirements?

([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/If-an-entity-uses-a-third-party-service-provider-TPSP-that-has-been-validated-as-PCI-DSS-compliant-is-the-entity-s-assessor-required-to-go-onsite-to-the-TPSP-s-location-and-retest-the-PCI-DSS-requirements/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/If-an-entity-uses-a-third-party-service-provider-TPSP-that-has-been-validated-as-PCI-DSS-compliant-is-the-entity-s-assessor-required-to-go-onsite-to-the-TPSP-s-location-and-retest-the-PCI-DSS-requirements/))

Source: <https://www.pcisecuritystandards.org/faqs/1576/>