

Can sensitive information be redacted from the PCI DSS Attestation of Compliance before it is shared with other entities?

PCI SSC FAQ | Article 1354 | April 2023

Yes, an entity may redact sensitive information from their PCI DSS Attestation of Compliance (AOC), providing that the resulting document contains, unredacted, all information relevant to the purpose for which the AOC is being shared.

While AOCs are intended to be shared, an AOC might contain sensitive information about the entity's internal environment or security implementation that is not relevant to every organization the entity shares their AOC with. For example, it may not be necessary for a servicer provider's customers to know the city where a data center is located, or details about the technologies present in the service provider's cardholder data environment (CDE). Conversely, details about the scope and services covered by the PCI DSS assessment, the requirements assessed, and the findings of the assessment, are relevant to the service provider's customers and should be included in the service provider's AOC.

Examples of AOC sections that should not be redacted because they include information relevant to the purpose of sharing AOCs include:

- Section 1: Part 1: Contact Information
- Section 1: Part 2a: Scope Verification (in Service Provider AOCs)
- Section 1: Part 2f: Third-Party Service Providers
- Section 1: Part 2g: Summary of Assessment
- Section 2: Report on Compliance/Self-Assessment Questionnaire
- Section 3: Validation and Attestation Details

Sharing the AOC may be preferred to sharing the full Report on Compliance (ROC) or Self-Assessment Questionnaire. However, for the AOC to serve its purpose, the information contained within must provide a meaningful summary of the assessed environment and, in the case of service provider AOCs, clearly identify the services covered by the assessment.

Where information relevant to the services offered is sensitive or confidential, entities may consider having a confidentiality agreement in place so that such information can be shared.

Entities providing a redacted AOC to a payment brand or acquirer for compliance validation purposes are advised to consult with the brand or acquirer for information about their reporting requirements, because requirements regarding redaction of AOCs can vary. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

See also FAQ #1220: Are compliance certificates recognized for PCI DSS validation?

Source: <https://www.pcisecuritystandards.org/faqs/1354/>