

Can the "Compliant but with Legal exception" option in the AOC be used to identify where a testing procedure could not be performed due to a legal constraint?

PCI SSC FAQ | Article 1486 | December 2020

No. The "Compliant but with Legal exception" option in Part 3 of an Attestation of Compliance (AOC) allows an entity to document that they could not implement one or more requirements because doing so would contravene a local or regional law or regulation. In such circumstances, the requirements that cannot be met must be marked as "Not in Place" in the accompanying ROC (Report on Compliance) or SAQ (Self-Assessment Questionnaire), as applicable. Use of the "Compliant but with Legal exception" option also requires additional review from the acquirer or payment brand to whom compliance is being reported.

Where the assessor is unable to complete testing of a requirement because of a legal constraint—for example, due to government enforced travel restrictions, local or regional lockdowns, or other factors impacting the assessor's ability to gain access or complete a testing activity—the affected requirements must be marked as 'Not Tested'. Because the assessor was unable to determine whether the requirement has been met, Part 3 of the AOC must be marked as 'Non-Compliant.'

In situations where testing procedures cannot be completed, assessors are encouraged to document in the report why the requirement could not be tested, and entities encouraged to consult with their acquirer and/or payment brand to understand expectations regarding partial or incomplete assessments.

Source: <https://www.pcisecuritystandards.org/faqs/1486/>