

Can a PCI 3DS Assessment result in a finding of "Compliant" if some requirements are not tested?

PCI SSC FAQ | Article 1490 | December 2020

No. The PCI 3DS Attestation of Compliance (AOC) can only document a "Compliant" finding if all requirements are tested and found to be "In Place" or a combination of "In Place," 'In Place w/CCW' (in place with compensating controls worksheet), and/or "N/A" (not applicable). Where the assessor has marked requirements as "In Place w/CCW" or "N/A," the assessor would also need to perform appropriate testing and complete the appropriate appendixes of the PCI 3DS Report on Compliance (ROC).

Version 1.0 of the PCI 3DS ROC and AOC do not include an option to report requirements as 'not tested'. Because the assessor has not determined whether such requirements could be applicable or whether they have been met, any PCI 3DS requirements that have not been tested must be marked as "Not in Place" and the overall compliance status marked as 'Not Compliant'.

Support for "not tested" responses is planned for inclusion in a future update to the PCI 3DS ROC and AOC. Requirements identified as "not tested" would also result in a finding of 'Not Compliant'.

Source: <https://www.pcisecuritystandards.org/faqs/1490/>