

Does a QSA need to be onsite at the client's premises for all aspects of a PCI DSS assessment?

PCI SSC FAQ | Article 1455 | January 2018

Per the QSA Qualification Requirements and QSA Program Guide, "QSA Companies and their QSA Employees" responsibilities in connection with the Program include, but are not limited to— Performing PCI DSS Assessments in accordance with the PCI DSS, including but not limited to— Being on-site at assessed entity during the PCI DSS Assessment.

PCI SSC intends for on-site testing to be the norm, with the majority of PCI DSS assessment testing completed at the physical client location. Though the entire PCI DSS Assessment may not require being on-site, required validation methods like "observe" — meaning the assessor watches an action or views something in the environment — are difficult to complete remotely. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions and physical controls.

Ultimately, the QSA is responsible for ensuring that any validation that is performed remotely is reasonably defensible, including that the remote validation is appropriate for the requirement being assessed and for each entity's particular implementation. For example, a QSA may request an onsite physical presence to observe physical security controls, attempting to "open doors," etc. Similarly, in some cases a QSA might have a convincing case for relying on screen shots provided to the QSA by the assessed entity – for example, if the QSA defined the system sample themselves and then directed the assessed entity's employee to specific settings while sharing a screen via conference call. Alternative ways to meet the onsite objective could include QSAs engaging qualified local QSA resources to do onsite visits on their behalf if it is not feasible for the primary QSA to travel to the onsite location, in accordance with the QSA program requirements related to sub-contracting. While most interviews should be conducted on-site, there may be scenarios where doing so may seem unreasonable and unnecessary. For example, it may not be reasonable for a QSA to fly to another country solely to conduct interviews on training in secure coding if the information obtained on-site at the primary and other locations describing the training is consistent with and supported by the answers provided by the employees by phone or video interview.

The QSA is expected to be physically on-site for each PCI DSS Assessment, though the duration of the on-site visit will vary. PCI SSC recognizes that outlier scenarios may exist where validation of individual requirements can be reasonably achieved remotely without on-site visit, but these are expected to be the exception and if such an approach is used, the QSA must be able to sufficiently document and defend why this approach was used for those individual requirements.