

What is the meaning of 'initial PCI DSS assessment'?

PCI SSC FAQ | Article 1485 | January 2024

Where an entity is being assessed for the first time against a PCI DSS requirement with a defined timeframe, it is considered an initial PCI DSS assessment for that requirement. This means the entity has never undergone a prior assessment to that requirement, where the assessment resulted in submission of a compliance validation document (for example, an AOC, SAQ, or ROC).

For an initial assessment against a requirement that has a defined timeframe (for example, with an activity that is to be performed once every three or six months), it is not required that the activity has been performed for every such timeframe during the previous year, if the assessor verifies that:

-
- The activity was performed in accordance with the applicable requirement within the most recent timeframe (for example, the most recent three-month or six-month period), and
-
- The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.

All other applicable PCI DSS requirements are expected to be in place at the time of the assessment.

If an entity has previously submitted a formal validation document, subsequent assessments of the requirements reviewed in prior assessments cannot be considered an initial assessment. Examples of situations that do not change or reset an entity's initial assessment date include where the entity:

-
- Misses a subsequent assessment date,
-
- Changes assessor companies,
-
- Reports to a different compliance entity, or
-
- Changes or introduces new technologies to the environment.

Where an entity is being assessed to a PCI DSS requirement with a defined timeframe for the first time—for example, if the addition of a new payment acceptance channel results in an additional PCI DSS requirement(s) becoming applicable or where a PCI DSS requirement(s) with a defined timeframe is added to a ROC or SAQ—the first assessment of the additional requirement(s) could be considered an initial assessment for that specific requirement(s).

Entities should always consult with their acquiring bank or payment brand(s) to confirm how to report their compliance. Contact information for the payment brands is provided in FAQ 1142 How do I contact the payment card brands?

Internal gap assessments and pre-production assessments that do not result in a formal compliance document are not considered initial assessments. For further guidance on PCI DSS compliance in pre-production environments, refer to FAQ 1333 Can PCI DSS compliance be determined by testing only pre-production environments using test data?

Source: <https://www.pcisecuritystandards.org/faqs/1485/>