

TREAT EVERY ASSESSMENT RESULT AS A CLAIM

In Place is not a mood, a screenshot, or a project update. It is a claim about a defined environment, period, control, and body of evidence that an assessor must be able to test.

PRACTITIONER POSITION

My practitioner position is that PCI DSS assessments are claims-based: every scope statement, applicability conclusion, testing result, and reporting status asserts something specific about an identified environment at an identified time. The useful discipline is to state the claim, its owner, its boundary, the expected testing procedure, the evidence population, the exceptions, and the conclusion before collecting attractive artifacts. 'Claims-based assessment' is practitioner vocabulary, not PCI SSC terminology, and it does not replace the PCI DSS testing procedures or reporting instructions.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A control owner supplies a policy, a dashboard screenshot, and a ticket showing that a security process exists. The assessment workbook marks the requirement In Place. Later, the QSA learns that the dashboard omitted two business units, the ticket covered only one quarter, and the policy described a workflow that was not operating for the full reporting population. The artifacts were real. The claim they were used to support was larger than the evidence.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- A requirement is marked In Place before the team writes the exact assertion being tested.
- Evidence is collected by document name rather than by the population, period, system, process, and expected control behavior it must demonstrate.
- One artifact is reused across several requirements without recording which distinct claim and testing procedure it supports for each use.
- Exceptions are removed from the presentation instead of incorporated into the claim, population, result, and remediation record.
- The assessed entity, evidence owner, reviewer, and assessor use the same words for materially different boundaries or time periods.

- A reviewer can locate the evidence but cannot reconstruct why it is relevant, sufficient, current, and specific to the assessed scope.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI DSS supplies requirements and testing procedures; the applicable reporting document records the assessor's results. PCI SSC FAQ 1566 reinforces the evidence boundary: the QSA is responsible for confirming that evidence is relevant to the assessment scope, directly related to the requirement, timely, and sufficient to support the assessor's opinion. A plausible document is therefore not automatically adequate evidence for the asserted result.

The claims-based model makes hidden disagreements visible early. A claim has a subject, scope, period, expected condition, test, evidence, exceptions, owner, reviewer, and disposition. If any of those fields are missing, the team has found assessment uncertainty before it becomes report-review debt.

This model also creates a disciplined role for automation and AI. Tools may inventory artifacts, connect records, identify population gaps, and draft traceability. They should not silently expand a claim, decide evidence sufficiency, or turn an unresolved exception into an assessment conclusion. Accountable people still own the representation, testing, judgment, and acceptance boundaries.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact statement are we asking the evidence to prove, for which environment and time period?
- 02 Which PCI DSS testing procedure and reporting field will evaluate or record this statement?
- 03 What is the complete population, and what confirms that the supplied evidence covers it rather than a convenient subset?
- 04 Which exceptions, contradictory records, or missing periods qualify the claim?
- 05 Who owns the underlying fact, who represents it, who tests it, and who records the final assessment result?
- 06 Could a new reviewer reconstruct the conclusion without relying on the original team's memory?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Extract every material scope, applicability, control-operation, evidence, and result statement from the engagement plan and workpapers. Rewrite vague labels as testable claims with a subject, boundary, and period.

02 / MAP

Connect each claim to its PCI DSS requirement and testing procedure, evidence population, artifacts, owners, exceptions, related claims, reviewer, and reporting destination.

03 / EXPLAIN

State why the evidence is relevant, direct, timely, and sufficient for this claim. Distinguish the assessed entity's representation, assessor testing, practitioner analysis, and compliance-program acceptance.

04 / REDUCE

Split oversized claims, remove duplicate evidence requests, stop reusing artifacts without lineage, and resolve population gaps before the conclusion is drafted.

05 / PROVE

Retain the claim ledger, population definition, evidence links, testing record, exception disposition, reviewer identity, dates, and final report reference as one reconstructable chain.

THE FIELD LAW

THE LINE WORTH REMEMBERING

AN ARTIFACT CAN BE AUTHENTIC AND STILL FAIL TO PROVE THE CLAIM MADE WITH IT.

Choose one In Place result and finish this sentence precisely: 'For this population, during this period, we tested this expected condition using this evidence and observed...' If the sentence collapses, the result is ahead of the proof.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0013 / PCI SSC Document Library / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0015 / FAQ 1566: Use of evidence obtained outside the current assessment / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-09 against canonical digest 2c39f075eac25ea079af18f75498fc4f44780400330568eeb334e4c1ad8fee73. Educational content, not a compliance determination. Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.