

CLAIMS-BASED ASSESSMENT: STATE THE PROPOSITION BEFORE YOU ASK FOR THE PROOF

An evidence request without a proposition creates a scavenger hunt. A report conclusion without a traversable claim creates an authority problem.

PRACTITIONER POSITION

My practitioner position is that a PCI DSS assessment is best operated as a governed system of bounded claims. "Claims-Based Assessment" is practitioner vocabulary, not PCI SSC terminology, and it does not replace PCI DSS requirements, testing procedures, reporting instructions, QSA professional judgment, assessed-entity representations, or compliance-accepting-entity authority. It makes the reasoning unit explicit. Each material proposition names the authority and claimant, subject and environment, relationship or behavior, population, period, expected condition, applicable source, test design, admitted evidence, observations, contradictions, limitations, disposition, report use, and reopening trigger. The assessed entity can state what it represents. The assessor can design and document the work that tests it. Reviewers can trace how evidence supports-or fails to support-the conclusion. A claims ledger stores these objects; evidence relationships connect them; the claims-based method governs how they move from assertion to accountable conclusion.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An entity says privileged access is reviewed quarterly. The portal contains an access-review screenshot, an exported user list, a ticket marked complete, a policy, and a manager's email. None states whether the claim covers human and workload identities, all CDE-connected systems, the entire quarter, terminated users, emergency accounts, inherited roles, provider support, or exceptions. The artifacts are real. The proposition is still unstable. Once the team writes the claim precisely, it discovers three distinct questions: the authoritative population was complete at the review cutoff; each required review occurrence happened within its window; and the resulting removals were completed and verified. One sentence became three claims, three tests, several evidence relationships, and one unresolved service-account population.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Evidence is requested by file name-policy, screenshot, ticket, scan-before the exact proposition and test are written.

- One requirement row carries a single green status even though it contains multiple environments, populations, control instances, periods, responsibilities, and exceptions.
- Entity representation, assessor observation, assessor judgment, report conclusion, and accepting-entity decision are written as if they were the same authority statement.
- A positive artifact is treated as proof of a negative claim such as no unapproved service, no stored PAN, no missed occurrence, or no alternate path.
- A sample exists without a complete population, variant model, selection rationale, tested items, exceptions, and inference boundary.
- Contradictory evidence is overwritten by the cleaner artifact instead of preserved as a claim state requiring disposition.
- The report sentence cannot be traced backward to the tested subject, population, period, evidence objects, exceptions, reviewer, and limitation.
- A reused artifact brings another framework's, another customer's, another period's, or another assessor's conclusion with it.
- The claim remains approved after architecture, responsibility, evidence source, control operation, or applicable guidance changes.
- The team believes a claims ledger is the method, when the ledger is only one register inside the larger assessment reasoning system.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Use the proposition as the unit of work. A requirement number is an authority reference, not always a complete assessment claim. One requirement can create many propositions across system components, service providers, implementations, populations, periods, occurrences, customized or compensating-control cases, and report responses.

Classify the claim before testing it. Useful classes include scope, applicability, eligibility, responsibility, implementation, configuration, capability, occurrence, population completeness, evidence provenance, test result, exception disposition, remediation completion, and report conclusion. The class exposes which facts, authorities, and tests the claim needs.

Keep the authority chain visible. PCI SSC publishes standards and guidance. The assessed entity represents its environment and operation. Service providers represent their services and evidence. The assessor performs testing and reaches professional conclusions. The compliance-accepting entity determines program acceptance. A software status or AI output may assist the work; it does not inherit any of those authorities.

Write the claim envelope before collecting evidence: stable claim ID and version; claimant; subject and environment; exact proposition; boundary and non-claims; applicable source; population and variants; period and cutoff; responsibility; expected test; expected evidence; known exceptions; reviewer; and reopening conditions. If those fields are unknown, the request should say so rather than disguising discovery as proof.

Design the test from the claim. Inspection, observation, interview, configuration review, technical test, sample, complete-population test, reconciliation, negative test, or corroboration each answers a different kind of question. The test must identify what result would support the proposition, what would contradict it, and where the conclusion must stop.

Admit evidence deliberately. An artifact may be authentic yet irrelevant, relevant yet outside the period, timely yet incomplete, complete yet unauthoritative, or useful only as corroboration. Record provenance, acquisition, represented subject and period, transformation, integrity reference, sensitivity, limitations, contradictions, retention, and the exact claims it may support.

Separate observation from conclusion. Expected, observed, documented, asserted, and validated states may all be true and still disagree. Preserve the disagreement. An exception, unavailable record, failed control occurrence, incomplete population, or adverse test result is assessment data-not an inconvenience to delete on the way to green.

Treat negative claims as work. "No PAN is stored," "no other public endpoints exist," and "no quarterly reviews were missed" require bounded populations, authoritative sources, alternate-path discovery, representative or complete testing, and explicit limitations. Absence from one console, interview, or search result is not proof of absence.

Compile conclusions instead of typing them from memory. The report statement should be a governed projection of current claim versions, tests, evidence, exceptions, dispositions, limitations, and authority. If a conclusion cannot be traversed backward, it is not ready for review merely because the prose sounds correct.

Make change reopen claims. Architecture, software, identity, service-provider, responsibility, control, population, evidence-source, requirement, guidance, incident, failure, exception, and assessment-period changes should identify affected propositions. Approval is a property of an exact claim version-not a lifetime achievement badge.

Use automation for joins and checks, not invisible judgment. Machines can detect missing fields, stale periods, broken links, untested variants, unresolved contradictions, and changed dependencies. They should not silently determine PCI DSS scope, applicability, control effectiveness, evidence sufficiency, report conclusions, or program acceptance.

Measure assessment quality by reproducibility. A qualified cold reviewer should be able to state the proposition, reconstruct the subject and population, understand the test, locate admitted evidence, see adverse facts and limitations, and explain the disposition without relying on the original assessor's memory.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 What exact proposition are we asking the evidence to support?

02 Who is making the statement, and what authority does that actor actually hold?

03 What subject, environment, relationship, implementation, population, period, and cutoff does the claim cover?

- 04 What does the claim explicitly not say?
- 05 Which PCI DSS source or other authority grounds the expected condition, and is that source current?
- 06 What test answers this claim, and what result would support, qualify, contradict, or stop it?
- 07 What is the complete population, what material variants exist, and why is any sample representative?
- 08 Which evidence objects were admitted, for which claim versions, with what provenance, period, limitations, and contradictions?
- 09 What did the assessor observe, what judgment was applied, and what remains an entity assertion?
- 10 How are failed occurrences, exceptions, remediation, and retesting represented without rewriting history?
- 11 Which report sentence or response consumes this claim, and can it be traversed backward?
- 12 Which change, source update, new fact, or acceptance direction must reopen the claim?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Choose one important report sentence or requirement response. Recover every implicit proposition, authority statement, subject, population, period, responsibility, test, evidence object, contradiction, exception, disposition, and downstream use hiding inside it.

02 / MAP

Give each proposition a stable versioned claim ID. Join it to subjects, relationships, obligations, population sources, tests, evidence objects, observations, contradictions, dispositions, conclusions, owners, reviewers, and reopening triggers without flattening their distinct authority.

03 / EXPLAIN

State the proposition and its non-claims in plain language. Describe why the selected test fits, what the evidence represents, which limitations remain, how adverse facts were treated, and where professional judgment begins.

04 / REDUCE

Replace duplicate requests and copied conclusions with references to authoritative claim, evidence, and test records. Split overloaded claims, retire superseded versions, and automate missing-link and stale-period detection while preserving accountable decisions.

05 / PROVE

Give the complete record to a qualified cold reviewer. Require a backward trace from report sentence to current claim version and a forward trace from one changed fact to every affected test, disposition, and conclusion. Preserve the first unsupported leap and smallest repair.

THE FIELD LAW

THE LINE WORTH REMEMBERING

NO PROOF WITHOUT A PROPOSITION. NO CONCLUSION WITHOUT A TESTABLE CHAIN. NO APPROVAL WITHOUT AN EXACT CLAIM VERSION.

Take one sentence from the assessment report and turn it into a complete claim stack: authority, subject, population, period, test, evidence, contradiction, disposition, conclusion, and reopening trigger.

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-0003 / Is sampling allowed in PCI DSS v4.x? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0008 / FAQ 1473: Role of compliance-accepting entities and assessors in determining applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0080 / FAQ 1566: Can a QSA ask an auditor from the same company to collect evidence for a PCI DSS assessment? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0081 / FAQ 1567: Can a QSA rely on results from a non-PCI DSS assessment? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0118 / FAQ 1569: Is sampling allowed in PCI DSS v4.x? / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / ASSESSOR_JUDGMENT / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-20 against canonical digest

128f5f804641caed60cebeefd75a084581911903e4b6d91321b1b9d90f503786. 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.