

EXPECTED VS. OBSERVED VS. DOCUMENTED VS. ASSERTED VS. VALIDATED

Five columns. One control. If they are all green, there is a fair chance somebody collapsed five different questions into one status.

PRACTITIONER POSITION

My practitioner position is that an assessment claim becomes intelligible only when five different states remain separately visible. Expected describes the applicable criterion, intended outcome, or designed state. Observed records what a person, tool, test, or system actually encountered at a bounded time, place, population, and method. Documented records what an artifact says-accurately, incompletely, historically, or otherwise. Asserted states the proposition an accountable party is asking another party to rely upon. Validated records the bounded conclusion reached after the criterion, subject, period, evidence, method, exceptions, and authority have been reconciled. These are not five maturity levels and they are not interchangeable labels for truth. A control can be well documented but not observed. A tool can observe a configuration that nobody has asserted satisfies a particular requirement. An owner can assert operation across a year while the evidence validates only one occurrence. A QSA can validate a bounded assessment claim without certifying that the future will remain unchanged. The useful work is not forcing every state to match. It is preserving where they differ, determining whether the difference matters to the exact claim, and naming the evidence or decision needed to resolve it. When a GRC platform turns expected, observed, documented, asserted, and validated into one green control status, it does not simplify the assessment. It hides the joins the assessment must test.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A policy says privileged access is reviewed quarterly. The identity platform export shows the current privileged population. A ticket contains one completed review from the fourth quarter. The control owner asserts that all four quarterly reviews operated. A dashboard marks the control effective because the ticket is attached and the latest export passed its configured check. The assessor can see five different objects: the expected quarterly obligation, a current observation, a document for one occurrence, an annual operating assertion, and no completed validation of the four-occurrence claim. None of the individual objects is necessarily false. The Wack appears when the system lets one object impersonate the others. The assessment needs stable identifiers for the control, population, occurrence, evidence, assertion, test, exception, and conclusion so the team can see exactly what is supported-and exactly what is not.

WHAT SHOULD MAKE YOU STOP

- The control record has one status but no separate fields for criterion, observed fact, document statement, accountable assertion, and validation conclusion.
- A policy or procedure is treated as evidence that the described activity occurred during the assessment period.
- A current configuration observation is stretched backward to support prior recurring occurrences without an explicit continuity argument.
- An attached artifact automatically turns the control green even though its subject, population, period, or result does not match the claim.
- The control owner is never asked to write the exact proposition being asserted, including scope and time.
- A scanner, GRC connector, or dashboard result is called validated without identifying the method, coverage, exceptions, reviewer, or decision authority.
- The assessor's conclusion is stored by overwriting the entity's assertion or the underlying observation.
- A failed observation disappears when a later passing observation arrives, leaving no explanation of the exposure interval or corrective work.
- The same word-implemented, effective, compliant, complete, or passed-means something different in policy, operations, tooling, and assessment views.
- Nobody can answer which mismatch would reopen the claim because the five states were never preserved independently.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Start with the expected state, but name its authority. The expectation may come from PCI DSS, program direction, entity policy, architecture standard, contract, service responsibility, or a practitioner recommendation. Those sources do not have identical authority, and an expected state is not evidence that the state exists.

Make observations atomic. Record who or what observed the fact, the exact subject and population, time, environment, method, query or test version, result, limitations, and raw reference. Observation is about what was encountered; it should not silently carry a compliance conclusion.

Treat documentation as a claim-bearing artifact, not a transparent window into operation. A policy can describe intent. A ticket can record an occurrence. A diagram can describe a boundary. An AOC can describe assessed service coverage. Each document supports only the propositions its content, authority, subject, and period can actually bear.

Require an assertion that can be tested. 'Control 7.2 is green' is not a useful proposition. 'All privileged access to these production CDE systems was reviewed by these accountable roles in each required quarterly occurrence during this period, with exceptions handled through this process' is closer to something

an assessor can evaluate.

Define validation as bounded reconciliation, not ceremonial approval. Identify the criterion, assertion, subject, population, period, evidence set, testing method, sampling rationale where used, exceptions, contrary evidence, reviewer, authority, and conclusion. A validated claim should state its limits and reopening triggers.

Preserve disagreement. Expected and documented may differ because the policy is stale. Documented and observed may differ because implementation changed. Asserted and observed may differ because the population is incomplete. Validated and asserted may differ because evidence supports a narrower period. The mismatch is assessment information, not interface clutter.

Do not model the five states as a one-way pipeline. Observation can reveal a new expectation. Validation can force an assertion to narrow. Documentation can be corrected without changing the observed system. A failed observation can be valid evidence of non-performance, corrective action, and later recovery.

Use time as a first-class key. Expected frequency, observed timestamp, document effective date, asserted period, and validation date answer different questions. One current screen cannot retroactively create a missing occurrence, and one historical artifact cannot automatically establish current operation.

Keep authority attached to every transition. The entity owns its representation. A TPSP owns its attestation and clarification. Tools emit observations. Assessors evaluate evidence and make assessment judgments. Compliance-accepting entities determine program treatment where applicable. A platform should not fuse those authorities into one anonymous status.

Build the assessment package from the joins. For each claim, show the expected criterion, relevant observations, governing documents, accountable assertion, validation work, exceptions, and unresolved contradictions. The result is not more paperwork. It is a smaller number of precise, reproducible claims with far less room for accidental overstatement.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 What exactly is expected, and which authority created that expectation?

02 What was actually observed, by whom or what, against which subject, population, environment, method, and time?

03 What does each document literally say, and what does it not say?

04 Who is making the assertion, what precise proposition are they asking others to rely upon, and for which period?

05 What validation work was performed, by which authority, against which criteria and evidence population?

06 Where do the five states disagree, and can the mismatch change the bounded claim?

07 Which occurrence, exception, failure, excluded population, or contradictory artifact remains visible after a later pass?

- 08 Does the validation conclusion support the full assertion, a narrower assertion, or no conclusion yet?
- 09 What source, system, owner, or method must change to resolve each mismatch without overwriting history?
- 10 Which event should reopen the validation: time, architecture change, population change, evidence failure, provider change, or new contrary observation?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Select one consequential control claim and collect the expected criterion, raw observations, governing and occurrence documents, accountable assertion, validation record, exceptions, failures, and contrary evidence without reconciling them in advance.

02 / MAP

Give every subject, population, occurrence, artifact, assertion, test, conclusion, and authority a stable identifier. Place each record in its proper state and connect only the relationships the evidence supports.

03 / EXPLAIN

Write the differences plainly: expected but not observed, observed but undocumented, documented but not asserted, asserted but not supported, or validated only within a narrower boundary. Keep source fact, entity representation, tool output, assessor judgment, and program direction distinct.

04 / REDUCE

Remove status words that conceal multiple propositions, stop auto-closing claims from attachments, narrow overbroad assertions, correct stale documentation, and design evidence emission around stable subjects and occurrences.

05 / PROVE

Reperform the traversal from criterion through observation, documentation, assertion, and validation. Confirm subject, population, period, method, authority, exceptions, and reopening triggers, then preserve any remaining mismatch as an open assessment fact.

THE FIELD LAW

THE LINE WORTH REMEMBERING

**EXPECTED IS A CRITERION. OBSERVED IS A FACT. DOCUMENTED IS A RECORD.
ASSERTED IS A CLAIM. VALIDATED IS A BOUNDED CONCLUSION.**

Download the Five-State Assessment Reconciliation Matrix. Take one green control and force its expected, observed, documented, asserted, and validated states into separate rows. The first unsupported join is the work.

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-0015 / FAQ 1566: Use of evidence obtained outside the current assessment / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0034 / Best Practices for Maintaining PCI DSS Compliance / 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 2026-09-10 against canonical digest

2e02e02dd828f51789ec9daed3b1d64b784f9d8fcccc230ee73f14f2607bc87d. 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.