

WHY DO I HAVE TO PROVE IT AGAIN?

You proved it last year. The assessor saw it. The ticket closed. Then the environment, population, period, owner, provider, or testing question changed. Which part of last year's conclusion do you believe survived unchanged?

PRACTITIONER POSITION

My practitioner position is that the demand to 'prove it again' is frequently described as audit repetition when it is actually a change-of-claim problem. Evidence is not permanently true because it was once accepted. It supports a bounded proposition about a subject, population, configuration, method, and period. When any of those dimensions changes-or when a new reporting period requires evidence of continued operation-the earlier conclusion may remain useful history but stop being sufficient current proof. PCI DSS also contains requirements with defined frequencies and activities triggered by significant change. Those obligations are not satisfied by the continued existence of last year's artifact. The disciplined question is therefore not 'Why does the assessor want the same screenshot again?' It is 'Which claim must be re-established, what changed, what stayed representative, and what new evidence is proportionate?' A mature assessment reuses durable evidence where its facts and period remain applicable, refreshes only the dimensions that changed, and records the rationale. An immature one either recollects everything mechanically or insists that historical acceptance created permanent immunity from reassessment.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A platform team supplied architecture, access, configuration, scan, and testing evidence during the prior assessment. This year it says the application is the same and asks why the package must be produced again. Since the prior review, the cloud account structure changed, a new identity provider became authoritative, the managed service added regions, two system components were replaced, the ASV target list changed, and several recurring controls reached new intervals. The visual interface still looks familiar. The underlying assessment proposition does not. Some durable records-approved design, ownership model, documented method-may remain applicable. Other records must show current configuration, current population, new occurrences, or post-change testing. Without a revalidation trigger matrix, both the entity and assessor are left arguing about document age instead of claim validity.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The team describes evidence as 'already accepted' without naming the claim, subject, population, configuration, and period it supported.
- A prior assessor's conclusion is treated as a permanent certification of the system rather than a conclusion bounded to an assessment and evidence set.

- Current-state exports replace recurring history, while design documents are recollected annually even though no design fact changed.
- Change tickets close without identifying which scope, control, testing, evidence, or reporting claims must reopen.
- The phrase 'no material change' appears without defined materiality criteria or a reconciled change population.
- Provider, version, tenant, account, region, identity, network, data-flow, or ownership changes are dismissed because the product name stayed the same.
- A GRC workflow requests the same artifact on a date but cannot explain whether the trigger is cadence, change, evidence expiry, or a new assessment period.
- The assessor requests a complete fresh package because neither party can determine which old records remain representative.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Treat evidence as a claim-bound object, not an annual collectible. It should identify what fact it supports, for which subject and population, under which configuration, during which period, using which method, and with which limitations. That metadata allows an old architecture decision to remain useful while a new access review, scan, or log-review occurrence proves continued operation.

Three different forces can require renewed proof. Recurrence creates a new required occurrence. Change can invalidate the representative value of earlier design or test evidence. A new assessment period asks whether the control continued to operate, even when the design stayed stable. Combining those forces into one generic expiration date produces busywork and missed obligations at the same time.

Prior acceptance is not a transferable shield. An assessment conclusion belongs to the facts, evidence, testing, professional judgment, reporting instructions, and acceptance context in which it was made. PCI SSC guidance on initial assessments reinforces that administrative changes such as changing the assessor or reporting entity do not simply reset assessment history. The inverse is also important: retaining the same assessor or artifact does not freeze the environment.

The right answer is not maximum recollection. Require a delta narrative: what changed, which identifiers and claims it touched, what durable evidence remains applicable, what new or updated testing is necessary, and who approved the rationale. This reduces Wack Tax because the assessment spends time on changed truth rather than identical file requests.

Build a Revalidation Trigger Matrix that joins change classes and time boundaries to affected claims. Include infrastructure, software, identity, data flow, providers, cryptography, segmentation, logging, scanning, penetration testing, ownership, evidence systems, and reporting instructions. A trigger should reopen only the connected claims-but it must not allow a changed dependency to disappear behind an unchanged system name.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact claim did the prior evidence support, and what were its subject, population, configuration, method, and period?
- 02 Which requirements create new occurrences or period evidence even when the design has not changed?
- 03 What changed in systems, software, identities, data flows, providers, networks, regions, controls, owners, or evidence retention?
- 04 Which change classes trigger additional scanning, penetration testing, inventory or diagram updates, or other revalidation?
- 05 Which durable records remain representative, and who documented that rationale?
- 06 Does a stable product name conceal a changed service, feature, tenant, version, deployment model, responsibility, or assurance boundary?
- 07 Can the assessment team distinguish evidence age from evidence applicability?
- 08 Can every reused conclusion be traced to an explicit unchanged-facts decision instead of convenience?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory the prior claims and evidence, the new assessment period, required recurring occurrences, and every relevant change since the evidence was tested. Use stable component, service, population, and claim identifiers so renamed files do not hide changed subjects.

02 / MAP

Connect each time boundary and change class to the claims, controls, diagrams, inventories, scans, tests, provider records, evidence, owners, and report sections it can invalidate. Record durable evidence separately from occurrence and current-state evidence.

03 / EXPLAIN

For every reused artifact, state why its subject, population, configuration, method, and authority remain representative. For every refreshed artifact, state whether recurrence, change, period, source update, exception, or acceptance direction reopened the claim.

04 / REDUCE

Stop asking for identical packages by calendar habit. Automate delta inventories, preserve historical occurrences, issue precise evidence contracts, and focus new work on changed or newly elapsed facts. Remove workflows that substitute file age for applicability analysis.

05 / PROVE

Sample both changed and allegedly unchanged claims. Trace changes to triggered testing and trace reused evidence to documented stability. Confirm that current diagrams, inventories, scan populations, penetration-test scope, provider responsibilities, and report language tell the same current-period story.

THE FIELD LAW

THE LINE WORTH REMEMBERING

YOU ARE NOT PROVING THE SCREENSHOT AGAIN. YOU ARE PROVING THAT THE CLAIM STILL DESERVES TO SURVIVE.

Download the Revalidation Trigger Matrix. Choose one artifact the team resents recollecting and identify its claim, period, stable facts, changed facts, trigger, and required response. If the only reason is 'annual,' the workflow needs more intelligence. If the only reason not to refresh is 'accepted before,' the claim needs more humility.

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-0032 / FAQ 1485: Meaning of an initial PCI DSS assessment / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0033 / FAQ 1087: Quarterly vulnerability scanning timeframes / 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 2026-09-09 against canonical digest

3fa834ae2b329a1fe46868f3233afcf9d0b8997ded18f5e58acfe7ba969c70d8. 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.