

YOUR OTHER-FRAMEWORK EVIDENCE IS NOT AUTOMATICALLY PCI DSS EVIDENCE

Please stop getting angry at the round hole. Your SOC report, ISO record, NIST workpaper, internal-audit test, cloud-assurance packet, or GRC attachment may be excellent evidence. It is not automatically evidence for the PCI DSS claim now being tested.

PRACTITIONER POSITION

PCI SSC FAQ 1567 says a QSA cannot rely on the result of a non-PCI DSS assessment because scope coverage and validation procedures vary. The FAQ does allow the underlying evidence to be considered after independent review of the relevant payment environment and account data, direct mapping to PCI DSS requirements, assessment timeframe and testing-procedure specifics, and whether the relevant PCI DSS controls are in place. FAQ 1566 preserves the QSA's ultimate responsibility for evaluating evidence even when another auditor collected it. Those are assessment boundaries, not a prohibition on reuse. My practitioner position is that cross-framework evidence reuse should be generous at intake and strict at admission. The artifact may travel; its former conclusion does not. Before it supports a PCI DSS claim, name the receiving claim, subject, environment, population, period, source, collection method, procedure, results, exceptions, limitations, and decision authority. Reuse what survives that translation. Repair what is incomplete. Collect what is missing. Do not blame PCI DSS, the other framework, the tool, or the assessor because a square artifact was presented as a round conclusion.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

The security team uploads a current SOC 2 report, an ISO 27001 control record, a NIST CSF status, a cloud-provider assurance packet, and an internal-audit workpaper. The GRC platform maps each object to PCI DSS requirements and turns several requests green. The artifacts may describe real controls and may save substantial collection effort. But one covers the corporate environment rather than the payment environment; one reports a service organization's conclusion without exposing the evidence needed for the entity's implementation; one uses a different population and period; one records a policy review but not the PCI testing procedure; and one omits an exception affecting a CDE-connected administration path. The team says the assessor is refusing perfectly good evidence. The assessor says the PCI claim is still unsupported. Both sides are staring at the same files through different claim boundaries.

WHAT SHOULD MAKE YOU STOP

- The answer to a PCI evidence request is the name of another framework, certification, audit, report, or dashboard rather than the bounded claim the artifact supports.
- A GRC mapping copies an achieved, effective, certified, clean, or passed status into PCI DSS without an independent evidence-admission decision.
- The artifact covers the enterprise, service organization, cloud account, or policy family, but nobody has reconciled the actual payment environment and account-data boundary.
- A report period, observation date, collection date, and PCI assessment period are treated as interchangeable clocks.
- A sample, selected control, or tested location from another engagement is reused without the complete PCI-relevant population and its material variants.
- The other engagement's objective and procedure are described as similar, but the PCI DSS requirement and applicable testing procedure have not been compared directly.
- The artifact's source, filters, transformations, exceptions, complementary responsibilities, limitations, or non-claims disappear when it is attached to the PCI request.
- The team expects a report-level conclusion to replace evidence of the assessed entity's actual implementation and operation.
- The assessor rejects an entire artifact without recording which admission gate failed, what portion remains useful, or the smallest evidence repair.
- The argument becomes framework versus framework even though the real mismatch is claim, scope, population, period, procedure, or authority.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Begin with the receiving PCI claim, not the donor framework. State the exact PCI DSS requirement or testing objective, the entity assertion, subject, environment, population, period, and conclusion still to be made. Evidence cannot be admitted to an unnamed claim. A familiar control family such as access control, vulnerability management, or change management is too broad to establish the receiving boundary.

Identify what the offered object actually is. A certification, attestation report, auditor opinion, policy, ticket, configuration export, interview record, test result, exception list, provider matrix, and dashboard are different objects. Preserve the publisher or source system, collector, collection method, represented state or period, transformations, version, integrity reference where appropriate, restrictions, and supersession relationship. The label evidence does not erase the object's original job.

Separate report reliance from evidence reuse. FAQ 1567 draws the central line: another attestation result is not a PCI DSS assessment result. Underlying evidence may still be useful after independent PCI-specific review. That means a clean SOC opinion, ISO certificate, NIST outcome, internal-audit conclusion, or vendor assurance statement can help locate facts without inheriting authority over the PCI conclusion.

Run the scope gate. Confirm that the artifact covers the relevant payment environment, account data, system components, people, processes, locations, provider services, and connected or security-impacting relationships. Enterprise-wide does not necessarily mean the CDE was included. Provider-wide does not necessarily mean the exact service or customer configuration was included. A narrower artifact may still be useful when its admitted subject is explicit.

Run the claim and procedure gate. Map the artifact to the exact PCI DSS requirement and applicable testing-procedure conditions. Compare objective, subject, criteria, method, frequency, expected observation, exception treatment, and conclusion language. Similar intent is not identical testing. If the donor procedure did not perform the receiving job, record the residual test rather than pretending the gap is philosophical.

Run the population gate. Name the complete candidate population, authoritative source, inclusion and exclusion rules, material variants, sample-selection method, and tested items. A sample selected for another engagement may not represent the PCI-relevant population. A reusable artifact that covers only one environment, identity path, provider service, or occurrence must not be stretched across the unrepresented variants.

Run the time gate. Distinguish the artifact's source-state time, represented period, collection time, other-engagement review period, PCI assessment period, and any PCI-specific frequency or occurrence requirement. Current is not a date. Annual is not a period. A valid artifact can be too old, too early, too late, or silent about operation during the period now being assessed.

Run the result-and-limitation gate. Preserve actual results, exceptions, qualifications, complementary responsibilities, exclusions, unavailable facts, contradictory evidence, and explicit non-claims. A useful object can be admitted as partial evidence. Partial is not failure; it is an honest boundary. The dangerous state is an object whose limitations were stripped away so that its green status could travel farther than its facts.

Record an admission disposition instead of an argument. Use admitted, admitted with residual testing, partial, context only, superseded, contradictory, or rejected. For every non-full disposition, state the failed gate, retained value, evidence gap, accountable owner, next action, and retest condition. The assessor should not merely say no; the entity should not merely say but we already passed this somewhere else.

Keep the authorities separate. The donor framework or report defines its own criteria and conclusion. The assessed entity owns its PCI facts, implementation representations, and evidence. The assessor performs the applicable PCI DSS testing and records professional judgment. The compliance-accepting entity determines acceptance under its program. A GRC platform can preserve mappings and admission records; it cannot promote a foreign conclusion into a PCI result by automation.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 What exact PCI DSS claim is this artifact being offered to support?

02 Does the artifact cover the relevant payment environment, account data, system components, services, people, processes, and relationships?

- 03 What donor-engagement objective and procedure produced the artifact, and how do they differ from the applicable PCI DSS testing procedure?
- 04 What is the complete PCI-relevant population, and were all material variants represented by the donor evidence or sample?
- 05 Which clocks describe source state, represented period, collection, donor review, PCI assessment, and required occurrence?
- 06 What did the artifact actually show, and which conclusion belonged only to the other framework, auditor, certifier, provider, or tool?
- 07 Which exceptions, exclusions, complementary responsibilities, qualifications, filters, transformations, and non-claims must travel with the object?
- 08 Can part of the artifact be admitted while a smaller residual PCI test closes the remaining gap?
- 09 Who records the evidence-admission disposition, who performs residual testing, and who retains final assessment and acceptance authority?
- 10 If the artifact is rejected, can a cold reader see the failed gate and smallest repair without reopening the entire framework argument?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Select one PCI request currently answered with another framework's report, workpaper, certificate, dashboard, or control record. Preserve the original object, source, objective, procedure, scope, population, period, result, limitations, and authority.

02 / MAP

Write the receiving PCI claim and compare claim, subject, payment scope, population, period, method, testing procedure, results, exceptions, limitations, and authority. Mark every exact match, partial match, unknown, and mismatch.

03 / EXPLAIN

Record what can be reused, what cannot travel, and why. Distinguish implementation reuse, underlying evidence reuse, residual PCI testing, donor conclusion, assessor judgment, and acceptance authority in plain language.

04 / REDUCE

Admit the portions that survive the boundary, reference the authoritative object instead of copying it, and define the smallest residual test or collection needed. Remove automatic status inheritance, unsupported equivalence, and duplicated requests.

05 / PROVE

Give the admission record and original artifact to a cold reviewer. Ask them to reconstruct the PCI claim, admitted evidence, failed gates, residual work, limitations, and authority boundary without oral rescue or a framework-versus-framework debate.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A REUSABLE ARTIFACT IS NOT A REUSABLE CONCLUSION. EVIDENCE BECOMES PCI DSS EVIDENCE ONLY FOR THE BOUNDED PCI CLAIM IT ACTUALLY SURVIVES.

Run the PCI Evidence Reuse Admission Record on one SOC, ISO, NIST, internal-audit, cloud-assurance, or GRC artifact. Reuse the facts that fit. Name the gap that remains. Stop asking a square conclusion to impersonate a round claim.

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-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 2026-09-18 against canonical digest

a1a582800c7374219920e3912cec5a35c8f166027d9581c7fbb96318a2019734. 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.