

THE EVIDENCE REQUEST IS A HUMAN API WITH TERRIBLE LATENCY

Ask for a screenshot, receive a file, discover the tenant is wrong, ask for the population, discover the period is wrong, ask what the file proves, and schedule another meeting. The latency is not caused only by slow people. The request had no contract.

PRACTITIONER POSITION

PCI DSS defines requirements and testing procedures; it does not prescribe a W/ evidence-contract template. PCI SSC FAQs 1566 and 1567 preserve the assessor's responsibility to evaluate whether evidence is specific to the assessment scope, directly related to the requirement, within the applicable timeframe and testing conditions, and sufficient to support the assessor's opinion. FAQ 1569 also makes the population visible when sampling is used: the sample must represent all population variants and be large enough to provide assurance across the population. My practitioner position is that many evidence cycles fail before evidence is collected. A request that names only a file type leaves subject, claim, population, period, source, method, response semantics, limitations, and acceptance boundary to be negotiated after transmission. Treat the request as a versioned human API contract: define the question and response envelope before files move; allow complete, partial, unavailable, superseded, and contradictory responses; preserve assessor follow-up and professional judgment; and route the accepted record into the claims ledger, evidence lifecycle, five-state reconciliation, and reporting work without pretending that contract conformance establishes compliance.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An assessor asks for 'the quarterly access review screenshot.' The entity sends a green dashboard. The dashboard covers production but not the support tenant. It shows the current result, not the quarter under review. The total excludes disabled accounts but the request never defined whether they belonged in the population. A spreadsheet arrives next, then a ticket, then four screenshots, then a meeting to explain the export. Each participant responded reasonably to a different implied question. The seventh exchange finally reveals the actual job: establish whether the defined account population for the named environment and period was reviewed, exceptions were dispositioned, and the tested evidence supports the bounded claim. The organization did not have an evidence shortage. It had a request-protocol failure.

WHAT SHOULD MAKE YOU STOP

- The request names a screenshot, export, policy, ticket, or report but does not state the bounded claim or testing objective.
- The entity cannot tell whether the request concerns one component, one environment, a complete population, a representative sample, or an example.
- The period is expressed as 'current,' 'latest,' or 'quarterly' without a start, end, occurrence, observation time, or timezone.
- The requested file is a convenient derivative, while the authoritative source, query, filters, exclusions, and transformation path remain unstated.
- Sensitive information is discovered after collection because the request did not declare minimization, transfer, retention, or redaction expectations.
- The response can only be 'uploaded' even when the evidence is partial, unavailable, superseded, contradictory, or dependent on another owner.
- Acceptance means the portal received a file, not that a named reviewer admitted it for a bounded purpose with explicit limitations.
- A clarification changes the claim or population but the request version, prior response, and affected downstream conclusions remain invisible.
- The same source is recollected for several requirements because no one records which bounded claims, populations, and periods it may support.
- The assessor's additional inquiry is treated as a process failure even when new facts legitimately require more evidence or a different test.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Start with the question, not the file. The request envelope identifies the requirement or testing objective, bounded claim, exact subject and environment, applicable period, complete candidate population, expected variants, requested test method, and conclusion that remains outside the request. 'Screenshot of MFA' is a file request. 'Evidence supporting whether MFA is implemented for the defined remote-access population during the assessment period' is a testable question.

Define the population before discussing the sample. Record the authoritative population source, inclusion and exclusion predicates, material variants, count or reconciliation method, and point in time. If the assessor samples, preserve the selected and represented items plus the rationale. A sample cannot repair a population that was never established, and a request contract cannot decide that a sample is sufficient on the assessor's behalf.

Separate the clocks. A durable request distinguishes control period, occurrence date, source-generated time, observation or execution time, collection time, submission time, and review time. One timestamp cannot silently answer every temporal question. If the request changes, create a new version and state

whether earlier responses remain applicable.

Name the authoritative source and the allowed response forms. The source may be a native configuration, API or CLI result, log, report, ticket, interview, observation, or document. The response may include screenshots, exports, transcripts, narratives, or corroboration, but every derivative keeps its source path, query, filters, transformations, collector, and limitations. The Screenshot Evidence Capture Record governs image-specific capture; the evidence contract governs why the capture was requested.

Give the response a vocabulary more honest than uploaded or missing. Complete means the declared envelope is addressed. Partial names the missing subject, period, population, field, or corroboration. Unavailable states the reason and owner. Superseded points to the current source. Contradictory preserves facts that do not agree. Clarification required identifies an ambiguity before a collector guesses. These are workflow states, not PCI DSS assessment results.

Make sensitivity part of the contract. State prohibited data, minimization rules, approved transfer path, original and derivative handling, permitted redaction, access, retention, and deletion or return obligations before collection. Never request PAN, sensitive authentication data, secrets, personal data, or restricted architecture merely to make the response look complete. If sensitive evidence is necessary, use the entity's approved handling process and retain the minimum needed for the defined job.

Separate delivery, admission, and evaluation. Delivery proves only that a response arrived. Admission records whether a named reviewer can use it for the bounded request, with which limitations and dependencies. Evaluation tests relevance, population, period, implementation, contradictions, and sufficiency. The assessor can reject, supplement, observe, interview, resample, or perform another procedure. A valid response schema is not an In Place conclusion.

Record non-claims. A current configuration export may not prove operation across a period. A policy may not prove execution. One successful event may not prove a complete population. A provider AOC may not prove the customer's implementation. A request that explicitly states these boundaries is shorter than the later argument caused by an unstated inference.

Route accepted evidence instead of renaming existing work. The Claims Ledger gives the bounded assertion an identity. Evidence Hygiene governs provenance, custody, retention, contradiction, reuse, and retirement. Screenshot Capture governs image attribution. Five-State Reconciliation keeps expected, observed, documented, asserted, and validated states distinct. The contract joins these methods at the request boundary; it does not replace them.

Measure latency by semantic round trips, not merely elapsed days. Count clarifications caused by missing claim, subject, population, period, source, field, sensitivity instruction, limitation, or decision owner. Distinguish legitimate follow-up caused by discovered facts from preventable follow-up caused by an incomplete request. The goal is not zero questions. The goal is to spend questions on assessment judgment instead of reconstructing the request.

Design for reuse without creating evidence laundering. A response may support several claims only when subject, population, period, source, method, and limitations fit each destination. Record the consumers and expiration trigger. Never copy a file into another requirement folder and infer that its meaning traveled with it.

Close the loop with a response decision. A named reviewer records complete, partial, unavailable, superseded, contradictory, clarification required, or rejected; states the reason; identifies the next action and owner; and names every claim or conclusion that remains open. New facts, a changed request, a changed population, source drift, period expiration, contradiction, or assessor challenge reopens the contract.

The protocol law is simple: every semantic field omitted from the request becomes a clarification round trip after collection. Better request design reduces Wack Tax, but it does not reduce the assessor's duty to challenge weak evidence or the entity's duty to explain what is actually true.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What bounded claim or testing objective is this request designed to inform?
- 02 Which exact subjects, environments, period, occurrence, and complete candidate population are in the envelope?
- 03 Which authoritative source establishes the population and which source establishes the observed condition?
- 04 If sampling is used, which variants exist, which items were selected, and who owns the sampling judgment?
- 05 Which response fields, formats, provenance, clocks, and corroboration are required before collection begins?
- 06 Which sensitive data must not be captured, and what approved handling applies to evidence that cannot be safely minimized?
- 07 Can the responder state partial, unavailable, superseded, contradictory, or clarification required without fabricating completeness?
- 08 Who admits the response for the bounded request, who evaluates it, and which decision remains outside both steps?
- 09 Which non-claims prevent a current setting, document, sample, or provider artifact from being stretched beyond its job?
- 10 Which existing claims, evidence records, reconciliations, workpapers, and report responses consume the admitted response?
- 11 What change to subject, population, source, period, implementation, contradiction, or request version reopens the record?
- 12 How many recent evidence loops were legitimate assessment inquiry, and how many merely reconstructed fields the first request omitted?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Select one high-friction evidence request and reconstruct every clarification, replacement file, meeting, and reopened question. Separate legitimate assessor inquiry from round trips caused by missing request semantics.

02 / MAP

Define the request envelope: objective, claim, subject, environment, period, population, variants, source, method, expected fields, response states, sensitivity handling, reviewer, consumers, non-claims, and reopening triggers.

03 / EXPLAIN

Issue the request in plain language and machine-readable fields where useful. Make delivery, admission, evaluation, and assessment conclusion distinct, and explain which existing governed method owns each downstream job.

04 / REDUCE

Remove ambiguous file labels, repeated collection, hidden filters, mystery clocks, binary upload states, uncontrolled sensitive data, and copied evidence. Keep legitimate follow-up and professional challenge visible rather than optimizing them away.

05 / PROVE

Run one fictional or safely sanitized request through complete, partial, and contradictory responses. Ask a cold responder and cold reviewer to reproduce the envelope, decision, next action, affected claims, and reopening condition without oral history.

THE FIELD LAW

THE LINE WORTH REMEMBERING

EVERY SEMANTIC FIELD OMITTED FROM THE EVIDENCE REQUEST BECOMES A CLARIFICATION ROUND TRIP AFTER COLLECTION.

Download the Evidence Request Contract and Response Record. Rewrite one recurring file request as a bounded question, run a partial or contradictory response through it, and count the clarification loops that disappear without weakening assessor inquiry.

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 2026-09-17 against canonical digest

f7e329cd28a4102191c195fb197a47f0c693b0cf502496dc66e5d0fbc95b5d78. 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.