

EVIDENCE HYGIENE IS NOT FOLDER HYGIENE

A beautifully named screenshot can still be anonymous, untimed, unbounded, transformed, and impossible to defend.

PRACTITIONER POSITION

PCI SSC FAQ 1566 says a QSA who uses evidence collected by another auditor remains responsible for evaluating whether that evidence is specific to the PCI DSS assessment scope, directly related to the requirement under review, within the assessment timeframe and any testing-procedure specifics, and sufficient to support an opinion about whether the relevant controls are in place. FAQ 1567 similarly says results from another attestation engagement cannot simply be relied upon for a PCI DSS assessment, although underlying evidence may be usable after independent review of scope, mapping, time, and whether relevant PCI DSS controls are in place. Those are assessment boundaries, not a prescribed metadata schema. My practitioner position is that evidence hygiene is the operating discipline that keeps an observation intelligible as it moves from its source into an assessment claim. It preserves identity, provenance, subject, population, time, method, original form, transformations, custody, sensitivity, relationship, review, supersession, retention, and disposition. A hash can show that bytes did not change after a known point; it cannot prove who created them, what population they represent, whether the source was complete, or whether a control was in place. A tidy folder can improve retrieval. It cannot repair missing context. Hygiene does not make weak evidence sufficient, and it does not authorize indiscriminate retention of sensitive data. It makes the evidence object reviewable, safely handled, and honest about what it can and cannot support.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A control owner uploads Q3-access-review-final2.png to a GRC platform. The folder is neat, the filename follows the convention, and the attachment has a green check. Six months later, nobody can say which identity tenant produced it, which roles or accounts were included, which query and filters were used, whether disabled accounts were excluded, whose local timezone appears in the screenshot, who redacted two rows, whether the uploaded image replaced the original export, or which review occurrence it was meant to support. The source link has expired. A nearly identical screenshot is attached to three requirements. The organization has excellent folder hygiene and poor evidence hygiene. The assessor is not looking at an evidence object with preserved boundaries. The assessor is looking at an orphaned picture of a conclusion.

WHAT SHOULD MAKE YOU STOP

- The filename is the evidence object's only durable identifier.
- An export or screenshot has no source-system locator, query, filter, collection method, or accountable collector.
- Created, observed, collected, uploaded, reviewed, and assessment-period dates are treated as one timestamp.
- The artifact says all, complete, quarterly, or current without a defined population, count, exclusions, or period.
- A redacted, annotated, converted, or cropped derivative overwrote the original instead of recording a visible transformation chain.
- A checksum is presented as proof that the source was authentic, complete, accurate, or sufficient.
- The same attachment is reused across requirements without a claim-specific coverage decision.
- Contrary, failed, late, incomplete, or superseded records live somewhere else-or quietly disappeared after a passing rerun.
- Sensitive exports are copied into shared drives or assessment portals without a classification, access boundary, retention basis, or disposal owner.
- The GRC platform shows attached and reviewed but cannot reconstruct what the artifact represented at collection time.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Begin at capture, not at upload. Assign a stable evidence ID while the source context is still available. Record the source system, tenant or environment, native object or report identifier, collection actor or service, collection method, query or configuration, and the relationship between the collector and the system being observed.

Separate the clocks. Preserve the period the control was expected to operate, the moment or interval actually observed, the source-generated timestamp, the collection timestamp, the upload timestamp, the review timestamp, and the timezone or clock basis that makes them comparable. A recent download can still describe stale operation.

Bind the population before celebrating the artifact. Name the systems, accounts, rules, events, occurrences, or other subjects the evidence purports to cover. Preserve population counts, selection logic, exclusions, exceptions, empty-result behavior, and the source from which completeness was evaluated. A screenshot of ten rows does not explain whether ten was the whole population or the visible page.

Preserve an original and make every derivative visible. Keep the native export or first defensible capture under controlled access. Record each crop, redaction, annotation, conversion, extraction, normalization, or aggregation as a new derivative with a parent identifier, operator, time, reason, and digest. Never force a

reviewer to guess whether the displayed artifact is original.

Use integrity carefully. A digest is valuable for detecting later byte changes when it is calculated and preserved at a known point in custody. It does not establish truth at the source, completeness of the query, authenticity of the actor, or relevance to a PCI DSS requirement. Integrity is one gate, not a conclusion.

Relate evidence to a precise claim and test. State which requirement or testing objective, subject, population, occurrence, period, method, and assertion the object may support. Then record contrary facts, limitations, and what remains unproved. Attachment presence should never auto-promote a claim to implemented, effective, or in place.

Preserve custody without manufacturing ceremony. Identify the accountable custodian, authorized viewers, transfers, transformations, reviewer, access restrictions, and system of record at a level proportional to sensitivity and dispute risk. The objective is reproducibility and safe handling-not a theatrical chain-of-custody form for every ordinary log extract.

Minimize and protect. Evidence hygiene includes collecting only what is necessary, avoiding unnecessary account data and secrets, using approved transfer and storage paths, controlling access, and defining a retention and disposal basis. More copies do not create more assurance. They create more uncontrolled surfaces and more contradictory versions.

Retain adverse history and supersession. A passing rerun may change the current conclusion but should not silently erase the failed occurrence, late execution, correction, or period affected. Link superseded objects to their successors, explain why the state changed, and identify which downstream claims must be reopened.

Make hygiene testable as business-as-usual work. Sample the register for orphaned files, missing boundaries, unverifiable transformations, expired links, uncontrolled sensitive content, duplicate identities, ambiguous timestamps, and unsupported claim links. The result is not a PCI DSS assessment. It is an operating control that gives the assessment a defensible evidence substrate.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What stable identifier follows this evidence object through every repository, portal, derivative, and assessment claim?
- 02 Who or what collected it, from which exact source, tenant, environment, object, query, filter, and method?
- 03 Which timestamps describe the source, observation, collection, upload, review, and assessment period-and in which timezone?
- 04 What complete population did the artifact address, how large was it, and which items were excluded or exceptional?
- 05 Is this the original, a derivative, or an aggregation, and can every transformation be reproduced from its parent?

- 06 What does the digest prove, and which authenticity, completeness, accuracy, relevance, or sufficiency questions remain open?
- 07 Which exact claim and test can this object support, and what does it not prove?
- 08 Where are the failed, contrary, late, incomplete, and superseded records for the same subject and period?
- 09 Does the object contain data that should be minimized, restricted, redacted, retained for a defined period, or defensibly disposed?
- 10 Can another qualified reviewer reconstruct the evidence boundary without asking the original collector what the file meant?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Select one frequently reused evidence object and collect its original source context, every stored copy and derivative, linked claims, review history, access boundary, and retention or disposal treatment.

02 / MAP

Give the object and each derivative a stable identity. Connect source, collector, method, subject, population, clocks, parent transformation, custodian, sensitivity, claim, test, exception, reviewer, supersession, and disposition.

03 / EXPLAIN

State exactly what the object observed, when, from which population, through which method, and under whose custody. Separate what its digest proves from what only source and assessment work can establish.

04 / REDUCE

Retire uncontrolled duplicates, preserve one governed original, create traceable derivatives, minimize sensitive content, replace expired links, and stop attachments from changing claim status automatically.

05 / PROVE

Reconstruct the object from source through transformation and claim use, confirm its boundaries against the relevant testing objective, and verify that exceptions, supersession, retention, and disposal remain visible.

THE LINE WORTH REMEMBERING

AN ORGANIZED FILE IS NOT HYGIENIC EVIDENCE UNTIL ITS IDENTITY, ORIGIN, BOUNDARY, TRANSFORMATIONS, CUSTODY, AND DISPOSITION ARE PRESERVED.

Download the Evidence Hygiene Intake and Custody Register. Choose the attachment your program reuses most and try to reconstruct its source, population, clocks, transformations, claim boundary, custody, and disposition without calling its original collector.

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](#)

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

Practitioner reviewed by Scott Norton on 2026-09-11 against canonical digest

a602166453da21c6b12c5a977cac59990af0a1305541d933517319277bc3d848. 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.