

SHOW ME THE FAILED WORK

If your evidence package contains only clean scans, completed reviews, resolved tickets, and perfect samples, I do not see a mature control environment. I see a story with the operating friction edited out.

PRACTITIONER POSITION

My practitioner position is that adverse evidence is not assessment debris. Failed scans, missed occurrences, incomplete populations, broken collectors, rejected changes, unresolved exceptions, false positives, late approvals, inconclusive tests, and corrective work are part of the control story. Their existence does not automatically determine a PCI DSS result; hiding, overwriting, or laundering them does make the assessment less reliable. PCI DSS testing asks whether requirements are in place, and the assessor must evaluate facts, populations, periods, exceptions, and corrective action according to the applicable reporting instructions and professional judgment. The assessed entity and assessor do not help the compliance-accepting entity by manufacturing a risk-free narrative. They help by presenting a bounded, attributable conclusion that makes deviations visible. A passing rescanning result is important, but it does not prove an earlier required scan happened on time. A completed review may demonstrate the current process, but it does not convert a missed historical occurrence into a completed one. A transparent evidence package preserves the before state, the failure, the response, the retest, the remaining limitation, and the effect on each claim.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

During readiness, a team cleans its evidence repository. Superseded scan reports are removed, failed jobs are rerun until green, exception tickets are exported only after closure, and the GRC platform shows the current final status. The intent is to reduce assessor confusion. Instead, the package loses the information needed to understand whether required activities occurred on time, whether failures were detected by the control or by the audit, whether remediation was prompt, whether rescans covered the same population, and whether a repeated issue indicates a design weakness. When the assessor asks for failed work, the answer becomes 'we only keep the final version.' The entity has optimized the repository for appearance and weakened it for assessment.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Only the final passing scan is retained; the original failure, remediation, and rescan chain is absent.
- The GRC platform overwrites status history or exports only the current green state.
- Missed control occurrences are recorded as completed using the date of later catch-up work.

- Exception records disappear from the assessment package once closed.
- Inconclusive, unavailable, excluded, or not-tested results are normalized to pass, not applicable, or no finding without a stated rationale.
- The assessment sample contains no failures even though operational teams remember remediation activity.
- A broken evidence collector is treated as a documentation problem without evaluating whether the control itself was observable or operating.
- Owners are coached to avoid discussing known gaps because they might 'create a finding.'

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Adverse evidence has multiple possible meanings. It may show that a preventive control failed, that a detective control worked, that governance identified a missed obligation, that a population was incomplete, or that the testing method could not support a conclusion. Those meanings must be evaluated, not flattened. A failed scan followed by remediation can demonstrate responsive operation while also preserving facts relevant to the original scan timing, vulnerability exposure, and requirement conclusion.

A clean final state is not the same as a complete assessment period. Defined-frequency activities have time boundaries. PCI SSC guidance states that periodic controls cannot simply be completed retroactively and backdated, and its scanning guidance distinguishes passing scans, remediation, and the consequence of failing to complete the required quarterly process. The record should therefore preserve both current correction and historical truth.

Transparency protects the compliance-accepting entity. An entity representation, assessor workpaper, ROC or SAQ response, compensating-control analysis, and accepting-entity decision may use different authority and judgment, but they must point to the same material facts. Removing adverse facts prevents the recipient from understanding what was tested, what changed, and what uncertainty remains.

Perfect packages also impair improvement. If operational failure disappears when the ticket closes, the program cannot measure repeated causes, late owners, fragile evidence paths, ineffective automation, population drift, or controls that require heroic manual rescue. The organization pays the same Wack Tax every cycle because it erased the data that could have redesigned the process.

Use a Failure-to-Claim Disposition Ledger. Give every adverse event a stable identifier and join it to the control occurrence, affected population, detection source, original evidence, immediate containment, root cause, correction, retest, residual limitation, affected claim, authority classification, reviewer, report treatment, and reopening trigger. The purpose is not to turn every failure into a public confession. It is to prevent the assessment from becoming fiction.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Which failed, missed, incomplete, excluded, inconclusive, or superseded records exist for the assessment period?

- 02 Did the control detect the condition itself, or did readiness or assessment activity discover it later?
- 03 Was the required activity performed within its defined window and against the correct population?
- 04 Does the retest cover the same subject and population, and what does it establish about the earlier interval?
- 05 Which original records were overwritten, discarded, or reduced to a final status?
- 06 How does each adverse fact affect entity representation, assessor testing, report language, and acceptance?
- 07 Which repeated failures indicate a control-design or operating-model problem rather than isolated operator error?
- 08 Can a reviewer reconstruct the complete sequence without relying on oral history?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory adverse evidence across scanners, ticketing, logging, identity, change, review, testing, provider, and GRC systems. Include missing and overwritten records as explicit gaps. Preserve original timestamps, artifacts, and population references.

02 / MAP

Connect each failure to its required occurrence, affected subjects and systems, control objective, evidence chain, corrective action, retest, assessment claim, reviewer, report treatment, and acceptance path. Distinguish detected control exceptions from failures of the control process itself.

03 / EXPLAIN

Write the chronology without euphemism: expected condition, observed condition, discovery source, timing, coverage, response, retest, current state, historical limitation, and claim impact. Keep entity representation, practitioner analysis, assessor judgment, and accepting-entity decision separate.

04 / REDUCE

Retain immutable history, prevent status overwrites, automate failed-job and missed-occurrence escalation, keep before-and-after evidence together, define exception taxonomies, and redesign recurring causes. Remove incentives that reward green dashboards for hiding unresolved work.

05 / PROVE

Sample adverse records as deliberately as passing ones. Verify original evidence, timing, population, ownership, correction, retest, recurrence, and report treatment. Confirm that the final conclusion preserves every material limitation and can be traced back to the unedited operating record.

THE FIELD LAW

THE LINE WORTH REMEMBERING

IF THE FAILED WORK CANNOT SURVIVE THE ASSESSMENT, THE PASSING WORK HAS NOT EARNED TRUST.

Download the Failure-to-Claim Disposition Ledger. Add the last five failed, late, incomplete, or overwritten control events before adding another green screenshot. If the team cannot show what failed, who knew, what changed, what was retested, and which claim moved, the package is polished-but not complete.

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-0031 / FAQ 1572: Periodic controls cannot be completed retroactively / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0033 / FAQ 1087: Quarterly vulnerability scanning timeframes / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0062 / FAQ 1152: Requirement to complete four passing quarterly ASV scans / 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

550ffc70df81856becdf716d2d3d3c7706f1d144354959ce33a3491a07369798. 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.