

NOTHING HAPPENED IS NOT EVIDENCE

No breach. No outage. No fraud anyone noticed. So why are you asking me to prove the control worked? Because a quiet year is an outcome, not a test of how the year was operated.

PRACTITIONER POSITION

My practitioner position is deliberately uncomfortable: 'nothing happened' is not evidence that a PCI DSS control was designed correctly, operated for the required period, covered the complete population, or produced the intended result. It is evidence of one observed outcome-the absence of a known event. That outcome can coexist with missing logs, unreviewed alerts, incomplete scans, untested access paths, stale inventories, and controls that failed silently. PCI DSS assessment is not a wager that the entity was probably safe because catastrophe did not arrive. It is an examination of defined requirements through stated testing procedures and applicable evidence. The entity should therefore separate control execution, control result, security outcome, and assessment conclusion. A clean incident register may support context. It cannot retroactively create the access review, scan, log review, change approval, inspection, test, or retained record that the operating model failed to perform. The useful response is not to manufacture proof. It is to disclose the gap, determine which claims the gap affects, correct the control, preserve the adverse history, and establish a repeatable evidence contract for the next occurrence.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An entity reaches the annual assessment with no reported account-data compromise and a dashboard showing green security posture. The assessor asks for recurring control evidence across the period. Several monthly reviews are missing, one administrative population was excluded from access review, and the internal scan console retained only the latest state. The control owners respond that there were no incidents and the tools would have alerted if anything important happened. Those statements may be sincere, but they collapse four different propositions: whether the control ran, whether it ran over the right population, whether exceptions were resolved, and whether the environment avoided a known adverse outcome. The absence of a known incident answers only the last proposition-and even that answer is bounded by the detection capability and records available.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The first defense of a missing control record is 'but we were never breached.'
- A green dashboard is offered without the underlying occurrence history, target population, exceptions, or retention limits.

- The team says a tool 'would have alerted' but cannot show that the relevant rule was enabled, fed complete data, monitored, and tested during the period.
- A current clean scan is used to imply that earlier required scans occurred and passed.
- An empty incident register is treated as evidence that preventive, detective, and response controls all operated effectively.
- Control owners can describe what normally happens but cannot identify dated occurrences, reviewers, inputs, outputs, or missed events.
- Missing evidence is recreated from memory, renamed from a later period, or summarized into a document that obscures the original gap.
- The assessment conclusion is written before the execution, population, exception, and outcome claims have been separated.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Separate the proof into four layers. Execution asks whether the required activity occurred. Coverage asks whether it addressed the right systems, accounts, locations, changes, or other population. Result asks what the activity found and how exceptions were handled. Outcome asks what happened to the environment. These layers can support one another, but they are not interchangeable. A favorable outcome does not prove execution; a completed task does not prove coverage; a clean result does not prove the method was capable of finding the condition.

Evidence absence must remain visible. Reconstructed context can explain what is known, but it should be labeled as reconstruction and should not be presented as a contemporaneous record. PCI SSC guidance on missed periodic controls makes the time boundary explicit: an activity required at a defined frequency cannot simply be performed later and backdated. Under bounded circumstances an assessor may evaluate the current and repeatable control state together with corrective action, but that professional judgment does not erase the missed occurrence.

The phrase 'no incidents' is only as strong as the detection system behind it. If logs were not retained, alerts were not reviewed, telemetry excluded relevant systems, or incident criteria were unclear, the entity may only be able to claim that no incident was recorded by the mechanisms that were operating. Precise language is not pessimism. It prevents a broad outcome statement from becoming unsupported evidence for unrelated controls.

Assessment pressure often creates the worst possible response: polish the narrative until the gap disappears. That creates a second failure. The original control weakness remains, and the evidence trail now misrepresents it. A mature program preserves failed work, missed work, superseded work, and corrective work because those records show whether governance can detect and change its own behavior.

The operating answer is a Control Outcome and Execution Map. For each material claim, record the required activity, accountable owner, due window, target population, method, contemporaneous evidence, result, exceptions, corrective action, security outcome, assessment use, and reopening trigger. This makes 'nothing happened' one bounded field in the story instead of the entire story.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact proposition is the phrase 'nothing happened' intended to support?
- 02 Which contemporaneous records prove that the control activity actually occurred in every required interval?
- 03 What population should have been covered, and how is completeness established independently of the result?
- 04 What did the control find, including failed, partial, unavailable, or inconclusive results?
- 05 Which exceptions were opened, assigned, corrected, retested, accepted, or left unresolved?
- 06 What detection and retention limitations bound the statement that no incident occurred?
- 07 Has any later document been presented as if it were an original in-period record?
- 08 Which assessment claims must remain pending, not in place, or otherwise qualified until the control has operated repeatably?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect the actual occurrence history, including successful runs, failures, omissions, partial populations, unavailable systems, alerts, exceptions, corrective actions, and evidence-retention gaps. Preserve timestamps and original records before writing the assessment narrative.

02 / MAP

For each control claim, map execution, population coverage, result, exception disposition, security outcome, evidence, owner, and period as separate objects. Show where one layer is present and another is missing rather than converting the whole row to green.

03 / EXPLAIN

State only what the records support. Distinguish no known incident, no recorded incident, control completed, complete population tested, exceptions resolved, and requirement concluded. Label reconstruction, representation, practitioner position, and assessor judgment explicitly.

04 / REDUCE

Replace fragile screenshots and annual memory exercises with retained occurrence records, stable population identifiers, automatic evidence capture, exception workflows, and owner-facing alerts for missing or incomplete work. Remove duplicate dashboards that hide the source state.

05 / PROVE

Select occurrences across the period, reconcile each to its expected population, inspect exceptions and corrective action, and test whether the control can detect both the intended condition and its own failure. Confirm that report language does not claim more than this chain supports.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A QUIET YEAR IS AN OUTCOME. IT IS NOT A SUBSTITUTE FOR THE WORK YOU WERE REQUIRED TO PERFORM.

Download the Control Outcome and Execution Map. Take the control everyone defends with 'nothing happened' and separate its occurrence, population, result, exceptions, outcome, and assessment claim. If one green sentence is doing the work of all six, the evidence story is not ready.

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-0034 / Best Practices for Maintaining PCI DSS Compliance / 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 c22bc43736623433da877662dc18fd5929704eaa2cb786a8dec2f403eaa80297. 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.