

RUN A PCI SCORCHED-EARTH ASSUMPTION RESET

Burn the inherited assumptions. Preserve the safeguards, records, and accountable decisions. Then make every PCI claim earn its way into the new model with current facts.

PRACTITIONER POSITION

My deliberately controversial practitioner position is that some mature PCI programs need a scorched-earth assumption reset: a controlled, parallel reconstruction in which no inherited scope conclusion, applicability decision, TPSP deferral, exception, diagram edge, evidence shortcut, or green status is accepted merely because it appeared in last year's assessment. The method destroys presumption, not production. It does not disable controls, erase evidence, discard required records, interrupt service, evade retention duties, or presume prior work was wrong. It preserves the operating environment and historical record while requiring each current claim to be restated with an owner, boundary, source, test, limitation, and reopening trigger. PCI Scorched Earth is practitioner shorthand, not PCI SSC terminology or a prescribed assessment method.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A program enters its seventh annual assessment with an impressive archive and an increasingly fragile explanation. The scope workbook was copied six times, the network diagram has annotations nobody can source, the same systems remain N/A for reasons written by former employees, provider responsibilities are inferred from AOC titles, and recurring evidence is attached to controls before anyone defines the population. Each artifact looks familiar. Together they create a self-reinforcing story in which prior acceptance is treated as current proof. Rather than edit another copy, the team opens a clean-room claim ledger beside the existing program and rebuilds the current story from observed architecture, accountable ownership, authoritative sources, and fresh evidence.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The strongest rationale for a current conclusion is that the same conclusion was accepted last year.
- Scope, applicability, and provider statements survive copy-forward even when the systems, services, owners, or data paths have changed.
- Teams defend familiar workbook cells before they can explain the current architecture those cells supposedly describe.

- Evidence is requested and uploaded against inherited control rows before the claim, population, period, and testing procedure are defined.
- Exceptions renew because their history is documented more clearly than their present necessity or exit conditions.
- No one can distinguish a PCI SSC source, compliance-program instruction, assessed-entity representation, assessor judgment, and practitioner recommendation in the inherited narrative.
- The prospect of rebuilding the fact model is treated as more dangerous than continuing to rely on unsupported conclusions.
- Historical records exist, but there is no controlled method for separating useful lineage from inherited presumption.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Copy-forward is efficient only when the carried claim is still true, appropriately bounded, and connected to current evidence. Without that test, the archive becomes an authority it never earned. One unsupported assertion can influence scoping, sampling, testing, remediation priority, provider reliance, and report language long after the original context disappeared.

A scorched-earth reset should create productive controversy because it removes the social protection of familiarity. Owners must explain why a conclusion belongs in the current model instead of pointing to its age. That pressure can reveal real control strength as readily as it reveals Wack: well-operated boundaries, explicit responsibilities, complete populations, and durable evidence should survive reconstruction quickly.

The method is intentionally conservative about change. The reset runs beside the current program, under normal change management, record-retention, legal, operational, and evidence-preservation obligations. Nothing is deleted or disabled to make the model cleaner. Differences become an adjudication queue. Accountable people decide which current facts replace, qualify, or reaffirm inherited claims, and the resulting lineage remains visible to reviewers.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which scope, applicability, responsibility, exception, evidence, and status claims exist only because they were copied forward?
- 02 For each inherited claim, what current architecture fact, authoritative source, accountable owner, testing procedure, and evidence population support it?
- 03 What historical evidence and decision lineage must be preserved even when a current claim is rejected or rewritten?
- 04 Which differences between the inherited program and the clean-room model require assessor judgment or direction from the compliance-accepting entity?

05 What operational, legal, retention, safety, and change-management guardrails prevent the reset from damaging production or the assessment record?

06 Which future changes should automatically reopen the reconstructed claim instead of waiting for the next annual copy?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Freeze a read-only snapshot of the current program and inventory every inherited scope conclusion, N/A decision, provider deferral, exception, diagram relationship, evidence claim, and status that the assessment depends upon.

02 / MAP

Build a parallel clean-room claim ledger from current inventories, diagrams, data flows, security-influence paths, services, owners, sources, populations, and observed system behavior. Do not use prior acceptance as evidence.

03 / EXPLAIN

Compare the inherited and reconstructed stories. Classify each claim as reaffirmed, qualified, replaced, unresolved, or escalated, and preserve the rationale, authority, reviewer, evidence, limitation, and history for the disposition.

04 / REDUCE

Retire unsupported assumptions and duplicated records through governed decisions. Narrow claims to what can actually be defended, while leaving production controls and retained evidence intact until authorized change or disposition is complete.

05 / PROVE

Select material claims and trace each one through current fact, applicable source, testing procedure, population, evidence, result, reviewer, and report language. Define the changes and evidence failures that reopen it.

THE FIELD LAW

THE LINE WORTH REMEMBERING

BURN THE ASSUMPTIONS. PRESERVE THE SYSTEMS, THE EVIDENCE, AND THE ACCOUNTABLE DECISIONS.

Choose one high-Wack domain - scope, TPSP reliance, N/A decisions, recurring evidence, or exceptions - and rebuild its claim ledger beside the current program. Do not delete a thing. Measure how many inherited conclusions survive on current facts alone.

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-0002 / How is an entity's PCI DSS compliance impacted by using TPSPs? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0005 / PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0008 / FAQ 1473: Role of compliance-accepting entities and assessors in determining applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0015 / FAQ 1566: Use of evidence obtained outside the current assessment / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

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

e10c008dd568bffd7b416eca311bbfe763e8f88a1b88c8c457371cee9b5276. 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.