

PCI DSS IS NOT THE ANACHRONISM. YOUR ASSESSMENT MACHINERY MIGHT BE.

The standard has moved toward continuous security, modern architectures, flexible control design, browser-side risk, and responsibly assisted assessment work. Many programs still ask dynamic systems to explain themselves through annual screenshots, flat spreadsheets, static diagrams, and compressed status labels.

PRACTITIONER POSITION

My practitioner position is that the strongest anachronism critique should not accuse PCI DSS of being obsolete. It should identify a representation gap. A familiar artifact becomes anachronistic when the organization treats the artifact as the operating truth after the environment has become more dynamic, relational, and observable than the artifact can express. Spreadsheets, screenshots, diagrams, interviews, documents, samples, and status labels still perform legitimate jobs. The failure begins when a proxy becomes the authority for facts it no longer continuously represents. PCI DSS v4.x expressly emphasizes evolving threats, continuous security, flexibility, modern architecture considerations, browser-side protections, and human responsibility when automation or AI assists assessment work. The useful challenge is therefore not to discard the required output. It is to connect each required output to attributable, versioned operating facts and preserve human judgment at the conclusion boundary.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A cloud-native payment service deploys several times each day. Infrastructure is defined partly in code, some provider-side settings remain outside that repository, short-lived workloads inherit identities and policies at runtime, public endpoints terminate at managed edges, and browser scripts can change independently of the application server. The assessment package still begins with last year's asset spreadsheet, a manually updated network diagram, screenshots of selected consoles, a flat provider-responsibility table, interview notes, and requirement rows marked In Place. Every artifact is useful. None can independently show that its population, relationships, configuration, period, owner, and limitations still match production. The problem is not that a spreadsheet, screenshot, or diagram exists. The problem is that the organization has no maintained translation from live facts to those assessment representations.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The annual assessment is treated as the control calendar rather than a validation of controls that operate throughout the year.

- An asset inventory lists components but cannot traverse their identities, routes, services, providers, owners, evidence, and security-influence relationships.
- A TPSP matrix says Customer, Provider, or Shared without naming the exact service, activity, configuration condition, retained customer verb, or proof source.
- A screenshot is accepted as self-explanatory even though its tenant, resource, population, filters, time, collector, authoritative source, and limitations are absent.
- A manually maintained diagram is asked to be the architecture authority for an environment already described more precisely by runtime, cloud, identity, DNS, repository, and provider records.
- A periodic review is performed to satisfy a clock even though the relevant state is continuously observable and deviations could be detected much earlier.
- Evidence collection begins with a broad request and ends with files rather than beginning with a defined claim, subject, population, period, source, method, and acceptance boundary.
- In Place, Not Applicable, Not in Place, or Not Tested becomes the primary stored fact instead of a bounded output derived from tested claims and attributable observations.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

The annual photograph is the first representational anachronism. Formal validation and reporting still have defined periods and outputs, but the control environment does not pause between them. The modern companion is not a permanently green compliance dashboard. It is an operating calendar of required occurrences, change-triggered reopening, retained exceptions, and evidence-producing events that makes the eventual assessment reproducible.

The flat inventory is the second. A row can name a component, but scope and testing depend on relationships: what the component does, where it runs, which identity changes it, which route exposes it, which provider supports it, what data or security influence crosses it, and which claims consume those facts. The modern companion is a governed relationship model that can still export the inventory rows an assessor or reporting template requires.

The flat responsibility matrix is the third. Customer, provider, and shared remain useful summaries, but they are not executable responsibilities. A defensible model names the exact service and the verbs: configures, operates, monitors, reviews, responds, changes, preserves, and proves. It also records conditions, evidence, limitations, and reopening triggers. The table remains; the graph behind it becomes explicit.

The anonymous screenshot is the fourth. Images remain useful for interfaces, observations, and human-readable context. They become anachronistic when they replace available source records or arrive without an evidence envelope. The modern companion is not screenshot prohibition. It is an attributable capture package joined to API, CLI, configuration history, logs, IaC, or other corroboration where those sources exist.

The document as reality is the fifth. Policies, procedures, narratives, reports, and workpapers remain necessary because organizations and assessors must explain meaning and judgment. But a document should describe or govern operation, not impersonate it. Runtime state, configuration, code history, identity

assignments, change records, and event streams can supply operating facts; accountable prose explains what those facts mean and where the conclusion stops.

The static diagram is the sixth. PCI DSS requires accurate diagrams and current data-flow representation; nothing about that objective requires the drawing application to become the system of record. The stronger direction is environment and governed facts to relationship model to human-readable diagram. A hand-maintained diagram can still be valid when it is reconciled. It becomes anachronistic when production has no obligation to tell it that something changed.

The calendar-only control is the seventh. Defined frequencies remain requirements, and continuous telemetry does not erase a required review, inspection, test, or human decision. The modern question is whether continuous observation can detect changed or failed state sooner, assemble the relevant population, and create an attributable occurrence for the required accountable action. Automation shortens detection latency; it does not silently perform judgment it cannot own.

The evidence request is the eighth. The classic workflow asks for a file and negotiates meaning afterward. An evidence contract reverses that latency: state the claim, subject, population, period, authoritative source, expected fields, method, freshness, sensitivity, limitations, reviewer, and reopening condition before collection. The assessor can still request additional evidence. The entity can stop treating each request as an archaeological expedition.

The requirement-by-requirement march is the ninth. Reporting is organized by requirement because recipients need a consistent validation instrument. Systems do not operate in that order. One workload can participate in network security, hardening, identity, vulnerability management, logging, testing, incident response, provider dependence, and governance at once. The modern companion is a bidirectional model: requirement to tested subjects and subjects back to every affected requirement and claim.

The compressed status is the tenth. In Place and the other reporting responses are necessary outputs, not sufficient knowledge models. A status should resolve from a traceable chain of requirement, objective, subject, applicability predicate, implementation, responsibility, evidence, observation, test, result, limitation, authority, and time. Keeping the chain does not weaken the report. It makes the report explainable when facts change.

The translation rule across all ten is conservative: preserve the legitimate job of the old abstraction, identify the facts it cannot represent, add a modern companion, and prove the projection back into the required PCI artifact. Do not replace spreadsheets with graphs nobody governs, screenshots with API dumps nobody interprets, interviews with automation nobody validates, or annual fire drills with dashboards that continuously overstate what they know.

This is why the claim matters: PCI DSS is not necessarily stuck in the past. The organization may be operating a modern standard through inherited assessment machinery. The repair is not rebellion against the Standard. It is a better connection between the current environment, the claims made about it, the evidence used to test those claims, and the formal output the compliance program requires.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which assessment artifact is currently treated as authoritative even though production can change without updating it?
- 02 What legitimate job does that artifact still perform, and what facts can it no longer express by itself?
- 03 Which runtime, configuration, identity, repository, provider, telemetry, or workflow source can supply the missing facts?
- 04 How is the complete population established, versioned, reconciled, and preserved for the relevant period?
- 05 Which facts require human observation, interview, interpretation, or professional judgment rather than automated collection?
- 06 Can a cold reader traverse from a reported status to the subject, implementation, owner, evidence, test, limitation, and decision authority?
- 07 When the environment changes, which inventories, diagrams, evidence contracts, test populations, responsibilities, and report claims reopen?
- 08 What proves the machine-readable source is complete, current, attributable, and specific to the assessed environment?
- 09 Which modern replacement would merely exchange one ungoverned proxy for another?
- 10 Can the program generate the required human-readable PCI artifact from maintained facts without pretending that generation is the assessment conclusion?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Choose one familiar assessment artifact and identify the exact decisions currently made from it. Separate its legitimate job from every authority or inference it has accumulated merely through habit.

02 / MAP

Join the artifact to the current subjects, relationships, authoritative sources, populations, periods, owners, evidence, tests, outputs, and change events it is expected to represent.

03 / EXPLAIN

State the representation gap: what the artifact proves, what it summarizes, what it cannot know, which modern companion supplies missing facts, and which conclusion still requires accountable human judgment.

04 / REDUCE

Remove duplicate manual transcription and ownerless snapshots. Preserve required documents and reports as governed projections over attributable facts, with visible exceptions and reconciliation failures.

05 / PROVE

Run one real or safely fictional change through the operating sources and every dependent PCI artifact. Confirm that the required output updates, the old state remains historically visible, and no automated projection claims more than the tested evidence supports.

THE FIELD LAW

THE LINE WORTH REMEMBERING

AN ARTIFACT BECOMES ANACHRONISTIC WHEN THE ENVIRONMENT CAN CHANGE WITHOUT CHANGING THE STORY THE ARTIFACT TELLS.

Download the Anachronism Translation Record. Choose one screenshot, spreadsheet, diagram, responsibility matrix, evidence request, or status row and prove its path back to current operating facts before replacing the tool that displays it.

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-0005 / PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0088 / FAQ 1317: What is meant by significant change in PCI DSS? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0116 / New Guidance: Integrating Artificial Intelligence into PCI Assessments / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0117 / Payment Page Security and Preventing E-Skimming / 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

6da1c3b2717de93b0cabd94e9c6a92d284cb03225ef5046a32ea156898781cf9. 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.