

STOP BUILDING GRC TOOLS THAT TREAT PCI AS A SECOND-CLASS CITIZEN

If a platform can map hundreds of frameworks but cannot explain one PCI scope boundary, evidence population, TPSP seam, or reporting conclusion, it does not support PCI. It stores PCI-shaped rows.

PRACTITIONER POSITION

My rebellious practitioner position is that PCI DSS should be a first-class product domain in any GRC platform that claims serious PCI support-not another framework overlay on a generic control catalog. PCI assessment work depends on environment-specific scope, system relationships, account-data flows, systems that connect to or can impact the security of the CDE, prescribed testing procedures, evidence populations and samples, recurring operational periods, TPSP responsibilities and evidence, applicability decisions, exceptions, and report-ready conclusions. A platform may choose a broader multi-framework strategy, but it should not market shallow requirement mapping as equivalent to supporting how PCI assessments are actually performed. This is practitioner analysis, not PCI SSC terminology or a claim about every GRC product.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A company buys a platform advertised as supporting dozens of frameworks. The PCI DSS requirements load correctly, control owners receive tasks, and evidence uploads attach to rows. Then the assessment begins. The team cannot relate requirements to the current CDE boundary, reconcile systems across diagrams and inventories, preserve evidence populations, record assessor-selected samples, distinguish provider and customer performance, carry exceptions into testing results, or generate a coherent ROC or SAQ story. The content library recognized PCI. The product model did not.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- PCI DSS appears as a licensed requirement catalog with the same fields and workflow used for every other framework.
- Scope is one project setting or asset tag rather than a dated relationship model covering the CDE, connectivity, security impact, segmentation, and change.
- Controls exist as reusable statements, but prescribed PCI DSS testing procedures and assessor results are not first-class records.

- Evidence means file attachment; population, period, source, collection method, completeness, sample rationale, exception, and retest lineage are optional prose.
- TPSP reliance is an inherited compliance badge rather than an exact-service responsibility and evidence model.
- The system cannot distinguish assessed-entity representation, assessor judgment, PCI SSC source, practitioner method, and compliance-accepting entity direction.
- Applicability, compensating controls, customized approaches, Not Applicable, and Not Tested are forced through one generic exception workflow.
- The dashboard can count completed controls but cannot reconstruct the claim, test, evidence, limitation, and reporting conclusion behind the color.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

The lowest-common-denominator GRC abstraction is attractive: frameworks map to controls, controls map to owners, owners upload evidence, and dashboards summarize status. That model can organize work. My practitioner position is that it becomes dangerous when a product treats the abstraction as the assessment itself. PCI DSS does not become testable merely because every requirement has a row and every row has a green status.

PCI is inconvenient for generic tooling because the important objects are relational and time-sensitive. Scope depends on architecture and security influence. Evidence depends on population, period, method, and result. Sampling depends on the assessed population and relevant variation. TPSP reliance depends on the exact service, responsibility, coverage, and residual customer work. Reporting must preserve what was tested, what was not, and why. These are product-model requirements, not decorative metadata.

The rebellious move is not to demand that PCI always outrank every business priority. It is to insist on product honesty. A platform can say that it provides catalog mapping and workflow support. If it claims PCI assessment support, it should demonstrate how the product maintains scope continuity, activity-level responsibility, prescribed testing, evidence lineage, assessor judgment, and report traceability without pushing the real assessment into side spreadsheets.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Can the platform represent the CDE, connected and security-impacting systems, segmentation, providers, and boundary changes as relationships rather than one asset tag?
- 02 Can each assessment result connect to the exact PCI DSS requirement and testing procedure, population, period, evidence, sample, exception, reviewer, and report location?
- 03 Can provider, customer, and shared activity be assigned at service level and reconciled to current provider evidence and customer testing?
- 04 Can the platform distinguish an assessed-entity claim, assessor test, practitioner recommendation, official source, and compliance-accepting entity instruction?

05 Can a scope, service, source, population, evidence, or control change identify the conclusions and publications that must be reopened?

06 What PCI work still moves into spreadsheets, diagrams, email, shared drives, or assessor-only workpapers because the product has no object for it?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory every PCI assessment activity performed outside the platform: scoping, architecture mapping, responsibility, population preparation, sampling, testing, evidence interpretation, exceptions, review, and report production.

02 / MAP

Connect those escaped activities to the missing product objects, relationships, states, roles, lineage, and change triggers-not merely to a list of desired screens.

03 / EXPLAIN

Separate catalog coverage, workflow support, evidence storage, assessment execution, and reporting support. State exactly which layers the platform provides and where accountable professional work continues elsewhere.

04 / REDUCE

Prioritize the missing domain capabilities that eliminate duplicate records and broken lineage: maintained scope relationships, claim-to-test chains, evidence populations, TPSP seams, exception/retest paths, and report traceability.

05 / PROVE

Run one realistic PCI result end to end. Show how a new scope fact, provider limitation, failed sample, or corrected artifact propagates to the affected test, conclusion, review state, and report language.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A FRAMEWORK CATALOG IS CONTENT. PCI ASSESSMENT SUPPORT IS A PRODUCT MODEL.

Ask your platform team for one demonstration: start with a new security-impacting system and show every scope, responsibility, testing, evidence, review, and reporting conclusion that the change reopens. If the demonstration ends in a spreadsheet, PCI is still a guest in the product.

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-0003 / Is sampling allowed in PCI DSS v4.x? / 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

b6810324760624e96453402f955041561a878277003b7a88deebd7fe385eb1e1. 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.