

Keeping PCI DSS Claims in Formation

The Diamond Fulcrum operating model for scope, applicability, responsibility, and evidence

Scott Norton | PCI DSS QSA | Johanson Group, LLP

PCI DSS assessment work becomes unreliable when scope, applicability, implementation, responsibility, and evidence describe different versions of the environment. The Diamond Fulcrum treats four claim positions as a formation around a versioned body of authoritative facts. It gives entities and assessors a practical way to detect drift, preserve independence, and propagate significant change across every dependent claim and artifact.

PRACTITIONER REVIEWED SOURCE

The Diamond Fulcrum is Scott Norton's independent practitioner model. It is not PCI SSC terminology or U.S. Navy doctrine and does not imply affiliation with or endorsement by PCI SSC, the U.S. Navy, or the Blue Angels.

Formation reference

Position	Job	Question
Scope	Reference	What environment and relationships does the assessment represent?
Applicability	Coupling	Which obligations connect to which subjects and tested facts?
Implementation and Responsibility	Execution	How does the activity operate and who performs each accountable verb?
Evidence	Support	What supports the claim for the correct subject, population, period, and procedure?

The assessment problem is formation drift

Many difficult PCI DSS engagements begin with artifacts that appear reasonable when examined alone. The component inventory names the application. The network diagram shows a connection. The provider packet identifies a covered service. A questionnaire marks several activities as inherited. Scan reports and screenshots sit in the evidence repository. The trouble appears when those artifacts are compared and they describe different versions of the environment.

That condition is formation drift. Scope may reflect the current architecture while the applicability response still reflects the prior payment flow. The responsibility matrix may name the provider while the customer configuration and retained activity remain undefined. Evidence may accurately show a control state that no longer exists. None of those problems can be repaired by making one spreadsheet more complete because the failure sits in the relationship among the claims.

My practitioner position is that PCI DSS assessment work should be treated as a coordinated claim system. Four positions must remain aligned: Scope, Applicability, Implementation and Responsibility, and Evidence. Each position has a different job. Each must resolve to the same authoritative environmental facts. When one moves, the others must be reconsidered.

The fact fulcrum

The fulcrum is the maintained body of facts about the environment. It includes assets, services, data flows, identities, locations, providers, responsibilities, configurations, occurrences, changes, and the relationships among them. These facts do not determine a compliance result by themselves. They give every scope statement, applicability response, operating assertion, and evidence claim a common reference.

A useful fact chain can be traversed. A payment API exists in production. A public hostname terminates at an edge provider. TCP 443 reaches an application service governed by a defined TLS policy. A workload identity calls a tokenization service. A managed deployment pipeline changes the application. Named teams own the service, access, provider relationship, and evidence. Each fact has a source, effective time, prior value, and reopening trigger.

The fact fulcrum prevents the requirement response from becoming the architecture source of truth. The direction should run the other way. Current facts support a bounded scope representation. The representation informs applicability analysis. Applicable activity connects to implementation and

accountable responsibility. Evidence supports the resulting claims for the correct subject, population, period, and procedure.

Position one Scope

Scope represents the people, processes, technologies, locations, account data flows, connected relationships, security influencing relationships, and third party services relevant to the assessment. Scope is not merely a circle placed around the systems that store account data. It is a maintained explanation of what exists and how the relationships matter.

A stale scope statement can be internally consistent and still reference the wrong environment. A management utility may no longer store cardholder data but may administer systems in the cardholder data environment. A webhook receiver may process only transaction references while remaining an Internet-facing payment boundary. A cloud identity platform may influence authentication and privileged access without appearing in a payment data-flow diagram. These relationships require analysis before a conclusion, not automatic inclusion or exclusion.

The Diamond Fulcrum makes the first test simple: can the entity identify the fact version on which the scope representation depends? If the inventory, diagrams, narratives, scan targets, test populations, and provider records cannot be reconciled to that version, the other positions are already flying against an unstable reference.

Position two Applicability

Applicability connects an obligation or reporting direction to a subject and a tested set of facts. It should preserve the predicate being evaluated, the source of direction, the response, the decision authority, and the condition that reopens the conclusion. Copying an answer from a prior assessment or validation instrument does not preserve that reasoning.

A new service, identity, feature, provider dependency, data path, or public interface can alter applicability without changing the requirement text. Conversely, the appearance of a requirement in an instrument does not settle every fact-specific applicability question. The analysis must retain the distinction among program direction, validation eligibility, requirement applicability, assessor judgment, and the decision of the compliance-accepting entity.

Formation integrity requires applicability to move when its factual predicate moves. A changed payment flow may reopen more than a single row. It may alter service inventories, third party reliance, testing populations, secure development obligations, access pathways, evidence expectations, and reporting statements.

Position three Implementation and Responsibility

Implementation describes how the activity operates. Responsibility identifies the accountable verbs. Who configures, operates, monitors, reviews, responds, changes, preserves, and proves? A provider may perform several of those verbs. The customer may retain others. Some activities may be shared. The model keeps those facts explicit instead of replacing them with a general statement that the vendor handles PCI.

Provider assurance remains important. An AOC and responsibility matrix can establish valuable facts about assessed services and allocated activities. They do not remove the need to identify the exact service in use, the customer's configuration, shared handoffs, assurance limitations, retained work, and the consequence of a contradiction or stale provider document.

The formation breaks when every team owns a component but nobody owns the relationship. It also breaks when the assessor becomes the person expected to define the entity's implementation. The assessed entity owns the operating representation. The assessor must independently evaluate whether the representation and evidence support the claimed result.

Position four Evidence

Evidence supports a bounded claim. It should identify the subject, population, period, source, method, limitations, contradictions, and reviewer. Volume does not repair a broken scope statement. A current screenshot does not prove operating history. A green dashboard does not establish population completeness. A provider report does not automatically establish the customer's use of the assessed service.

Evidence should arrive with enough provenance for another reader to reconstruct why it matters. Configuration evidence can support a point-in-time state. Logs and tickets may support recurring operation. Interviews and observation explain process behavior. Testing evaluates a proposition under declared conditions. Each object has a useful job, and problems begin when the object is reused to support a materially different claim.

When evidence contradicts the asserted implementation, preserve the contradiction. The assessment conclusion stops where support ends. The contradiction may reveal an evidence defect, a stale assertion, incomplete population, implementation failure, or fact change. The Diamond Fulcrum does not decide which explanation is correct. It makes the unresolved relationship visible and attributable.

The assessor validation orbit

The assessor remains outside the entity-owned formation. Examination, observation, interview, testing, and corroboration evaluate the claims, but they do not transfer ownership of the environment or compliance program to the assessor. The entity should be able to explain the systems, relationships, applicable activities, control behavior, responsibility allocation, and evidence before the assessor reconstructs them.

This separation protects both parties. The assessed entity retains accountability for operating and representing its environment. The assessor retains independence and professional judgment. The compliance-accepting entity retains its authority over acceptance and reporting direction. A strong engagement makes those boundaries visible instead of allowing a single workbook to blur them.

A useful test is whether the formation can survive removal of the assessor. If inventories stop changing, evidence stops accumulating, responsibility becomes unclear, and applicability decisions disappear when the assessment team leaves, the assessment has become the compliance program.

Significant change as a formation maneuver

A significant change begins with a changed fact. A new public endpoint, service, provider feature, identity, configuration, application path, or deployment method alters the environment. The entity should record the changed subject, relationship, effective time, owner, source, prior value, and expected consumers of that fact.

The next move is claim reopening. The team identifies every scope, applicability, implementation, responsibility, and evidence statement that depends on the changed fact. It then refreshes the consumers: inventories, diagrams, data-flow narratives, provider records, access models, scan

populations, penetration test propositions, secure development records, operating obligations, evidence contracts, and report responses.

The final move is validation. The team tests the new formation, preserves contradictions, records the accountable disposition and limitations, and defines the condition that will reopen the decision again. The objective is not synchronized paperwork for its own sake. The objective is synchronized claims about one environment.

A Tuesday operating model

The Diamond Fulcrum becomes useful when it operates between assessments. Product, infrastructure, identity, provider, and application changes update the fact fulcrum. The four positions reconcile to the new version. Applicable recurring activities produce occurrences. Those occurrences emit evidence. Contradictions, missed work, and exceptions reopen claims and decisions.

This is where the model connects to business as usual. A claims ledger links the proposition, subject, period, evidence, reviewer, disposition, and reopening trigger. A scope graph preserves relationships. A responsibility record names accountable verbs. The publication or assessment report becomes a governed projection of these operating records instead of the place where the organization tries to remember the year.

The practical objective is not a perfect formation that never moves. Modern payment environments change. The objective is a formation that moves deliberately, records why it moved, keeps every claim aligned to the current fact version, and shows where uncertainty still remains.

The practitioner position

PCI DSS obligations should not be assessed as isolated rows. Each applicable obligation belongs to a subject, implementation, owner, period, procedure, and body of evidence. Those relationships must remain in formation with the environment the assessment describes.

The Diamond Fulcrum gives teams a compact question for every change and every assessment claim: do Scope, Applicability, Implementation and Responsibility, and Evidence still resolve to the same authoritative facts? If the answer is unclear, mark the uncertainty, name the owner, test the relationship, and stop the conclusion where support ends.

That is the way out of the Cluster of Wack. Find the changed fact. Map the affected claims. Explain the accountable relationships. Reduce duplicated or unsupported assertions. Prove what remains.

Sources and authority

- PCI DSS v4.0.1 and current PCI SSC guidance remain the authoritative sources for PCI DSS requirements and assessment procedures.
- PCI SSC FAQ 1473 informs the discussion of scope and applicability validation.
- PCI SSC FAQ 1566 informs the discussion of evidence specificity and assessor responsibility.
- Official Blue Angels history and the 2026 Maneuvers Manual ground only the four-aircraft formation reference.
- The Diamond Fulcrum is Scott Norton's independent practitioner model. It is not PCI SSC terminology or U.S. Navy doctrine and does not imply affiliation with or endorsement by PCI SSC, the U.S. Navy, or the Blue Angels.