

THE BLUE ANGELS DIAMOND FULCRUM OF PCI DSS

PCI DSS is not a catalog of obligations flying independently. It is a formation whose claims must remain aligned with authoritative facts about the environment.

PRACTITIONER POSITION

The Blue Angels Diamond Fulcrum is a Cluster of Wack practitioner model inspired by the Blue Angels' four-aircraft Diamond formation. The official Navy sources establish that the Diamond is a real formation and identify its history and maneuvers; they do not define this PCI DSS analogy. In this model, Scope establishes the reference, Applicability stays coupled to scoped facts, Implementation and Responsibility explain how and by whom obligations are performed, and Evidence substantiates the bounded claims. The fulcrum is not another control category. It is the maintained body of authoritative environmental facts-assets, services, account-data flows, identities, locations, providers, responsibilities, configurations, occurrences, changes, and relationships-from which the formation is reasoned. The assessor remains outside the formation: the entity owns its environment, representations, implementations, and evidence; the assessor examines and tests whether the presented formation is accurately defined, documented, and supported. The model is practitioner analysis, not PCI SSC terminology, U.S. Navy doctrine, or a claim of affiliation or endorsement.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A payment API is recorded as Internet-facing, deployed in Azure, fronted by Cloudflare, reachable over TCP 443, configured for TLS 1.3, administered through Entra ID, connected to a tokenization service, and changed through a managed pipeline. The inventory lists the API. The diagram shows the connection. The provider packet names covered services. The requirement spreadsheet says several activities are inherited. The scan population omits the public termination, and the evidence folder contains a screenshot from the prior configuration. Every artifact can appear reasonable on its own. The formation breaks because the same authoritative facts do not resolve consistently across scope, applicability, responsibility, implementation, testing population, and evidence. One changed fact has created a multi-requirement maneuver, but only one document moved.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The component inventory, network diagram, data-flow narrative, testing populations, provider matrix, and requirement responses describe different versions of the environment.

- A system is added, removed, exposed, reconfigured, or delegated without reopening applicability and evidence decisions.
- Evidence is accepted because it exists, even though its subject, period, population, configuration, or owner no longer matches the asserted implementation.
- A provider performs an activity, but the exact service, customer configuration, shared responsibility, assurance evidence, and retained customer work are not joined.
- The requirement response drives the architecture story instead of authoritative facts driving the bounded response.
- A significant change updates the diagram but not scans, penetration-test propositions, identities, logs, policies, inventories, or report claims.
- The assessor is expected to construct the entity's formation rather than validate the entity's attributable representation.
- A green dashboard hides contradictory expected, observed, documented, asserted, and validated states.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Aircraft one is Scope. Scope is the reference from which the other positions are reasoned: people, processes, technologies, locations, account-data flows, connected or security-impacting relationships, and third-party services. It is not a circle drawn once for the assessment. If the factual reference is incomplete or stale, every downstream conclusion can be precisely documented and still be aligned to the wrong environment.

Aircraft two is Applicability. Applicability is not copied from a questionnaire row and it does not float free of the subject. It connects the scoped fact, requirement or reporting direction, applicability predicate, tested fact, response, authority, and reopening trigger. A new service, feature, identity, data path, or provider relationship can change the predicate even when the requirement text has not changed.

Aircraft three is Implementation and Responsibility. The formation needs the actual control behavior and the accountable verbs: who configures, operates, monitors, reviews, responds, changes, preserves, and proves. Provider performance can move work, but it does not erase the entity's need to identify the exact service, customer-controlled conditions, shared activities, assurance limitations, and retained responsibilities.

Aircraft four is Evidence. Evidence supports a defined claim about a defined subject, population, period, and procedure. It is not the formation leader and it cannot repair a broken scope or responsibility statement merely by being voluminous. Configuration, logs, tickets, reports, interviews, observations, screenshots, and tests become useful when their provenance and limitations stay attached to the claim they support.

The Fact Fulcrum is the shared reference plane beneath all four positions. A useful fact chain is explicit enough to traverse: payment-api-01 -> production -> public hostname -> edge provider -> TCP 443 -> TLS policy -> workload identity -> tokenization service -> deployment pipeline -> accountable owners -> retained occurrences. Facts are not assessment results. They are the versioned, attributable material from which scope and implementation are represented and against which an assessor can test.

Formation integrity is a reconciliation discipline. When Scope moves, ask whether Applicability moves. When Applicability moves, reopen Implementation and Responsibility. When Implementation changes, refresh the evidence contract and testing populations. When Evidence contradicts the asserted implementation, preserve the contradiction and stop the conclusion at the point the support ends.

A significant change is a formation maneuver, not a paperwork event. The change record should identify the authoritative facts that changed and fan that change into inventories, diagrams, provider relationships, identities, policies, scan targets, penetration-test propositions, recurring obligations, evidence expectations, report responses, and named decisions. The objective is not synchronized documents for their own sake; it is synchronized claims about one environment.

The assessor is not one of the entity's aircraft. PCI SSC FAQ 1473 places responsibility on assessors to validate that assessment scope and requirement applicability are accurately defined and documented. FAQ 1566 reinforces that a QSA must evaluate whether collected evidence is specific to scope, directly related to the requirement, within the relevant timeframe and testing conditions, and capable of supporting an opinion. The entity must still own the facts, representations, operations, and evidence it presents.

The BAU flywheel keeps the formation current. Changes update the fact fulcrum; the four positions reconcile; applicable operating obligations create occurrences; evidence is emitted and tested; contradictions and exceptions reopen decisions; and the resulting assessment determination remains attributable to a human. The practical objective is not to make 260-plus green rows. It is to keep every applicable obligation in formation with the current facts of the environment.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact, versioned environmental facts does each scope statement rely on, and where are those facts maintained?
- 02 Can every applicability response be traversed back to a subject, predicate, source of direction, tested fact, authority, and reopening trigger?
- 03 For each applicable activity, who performs, configures, monitors, changes, responds, and supplies evidence-and which verbs are shared with a TPSP?
- 04 Does every evidence object identify its claim, subject, population, period, source, method, limitations, contradictions, and reviewer?
- 05 Which single fact changes would move more than one position in the formation?
- 06 When did the four positions last reconcile to the same architecture and configuration version?
- 07 Which inventories, diagrams, scan populations, penetration-test propositions, policies, provider records, and report statements fail to move when the architecture moves?
- 08 Is the assessor validating an entity-owned representation, or quietly being asked to create it?
- 09 What can the current formation support, what remains W/? , and who has authority to decide the unresolved part?

ESCAPE THE WACK

01 / FIND

Choose one consequential payment capability and identify the exact authoritative facts that describe its current data, influence, identity, provider, configuration, change, and evidence relationships.

02 / MAP

Place the capability into four explicit positions-Scope, Applicability, Implementation and Responsibility, and Evidence-and draw every dependency back to the same fact fulcrum.

03 / EXPLAIN

Write one bounded claim for each position, name the accountable owner and authority, and state where the assessor's validation begins and the entity's representation remains its own.

04 / REDUCE

Remove duplicated facts, copied conclusions, ownerless provider deferrals, stale evidence, and document-only updates; preserve one attributable source for each fact and deliberate projections for each consumer.

05 / PROVE

Inject one significant change, identify every position and downstream artifact that must move, reconcile the resulting claims, and retain the test, contradiction, disposition, and reopening trigger.

THE FIELD LAW

THE LINE WORTH REMEMBERING

YOU DO NOT ASSESS HUNDREDS OF OBLIGATIONS IN ISOLATION. YOU ASSESS WHETHER EVERY APPLICABLE OBLIGATION REMAINS IN FORMATION WITH THE FACTS OF THE ENVIRONMENT.

Open the Diamond Fulcrum centerpiece and download the Formation Alignment Record. Run one real architecture change through all four positions before expanding the model.

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-0008 / FAQ 1473: Role of compliance-accepting entities and assessors in determining applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0080 / FAQ 1566: Can a QSA ask an auditor from the same company to collect evidence for a PCI DSS assessment? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0111 / Blue Angels History: Significant Events / United States Navy Flight Demonstration Squadron / [Open source](#)
- WACK-SOURCE-0112 / 2026 Blue Angels Maneuvers Manual / United States Navy Flight Demonstration Squadron / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / ASSESSOR_JUDGMENT / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-16 against canonical digest

afd7ad277bc7044e41333601f0377105268a9739a615357f2edc69ed23232e6f. 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.