

Diamond Fulcrum Formation Break

The webhook that moved only one document

45 MINUTES · ONE FICTIONAL CHANGE · FOUR POSITIONS · TEN CONSUMERS

Test whether one changed payment fact causes Scope, Applicability, Implementation and Responsibility, Evidence, and their downstream consumers to move together.

WORKSHOP BOUNDARY

This fictional practitioner exercise exposes dependencies, contradictions, and unsupported claims. It does not decide PCI DSS scope, requirement applicability, compliance, validation eligibility, provider responsibility, or acceptance. Use fictional or sanitized information only. Working notes remain on the device unless the participant downloads them.

Scott Norton | PCI DSS QSA | Johanson Group, LLP

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.

Run the break. Observe the method.

TIME	MOVE	FACILITATOR INSTRUCTION
00–05	Freeze the baseline	Read the facts without repairing them. Name the current authoritative fact version.
05–12	Fly four positions	Record one bounded claim and one unresolved question for each position.
12–15	Inject the change	Reveal the serverless function, workload identity, and support queue.
15–27	Move the consumers	Classify each downstream artifact as move, reopen, or hold with a stated reason.
27–35	Reconcile contradictions	Name the first stale relationship, unsupported claim, and ownerless verb.
35–41	Bound the disposition	State what is supported, what remains unresolved, who owns the next fact, and what reopens the decision.
41–45	Observe the method	Capture the first missed dependency, oral rescue, smallest repair, and retest condition.
THE ONE RULE Do not repair the scenario while reading it. Record the first dependency the room misses and the first explanation the facilitator has to supply.		

Do not collect

Names, email addresses, cardholder data, credentials, client evidence, restricted architecture, or real assessment findings. Use the anonymous observation page.

The webhook that moved only one document

- 01 Northwind Market uses a hosted checkout supplied by a payment service provider.
- 02 A production payment-status webhook is exposed through the entity's cloud edge service.
- 03 The application inventory and architecture diagram name the new endpoint.
- 04 External vulnerability and ASV scan target records still list the prior public addresses.
- 05 The penetration-testing methodology does not describe webhook behavior or its trust boundaries.
- 06 The provider responsibility record describes payment processing but does not identify callback delivery or customer receiver operation.
- 07 A screenshot from staging is attached to a production control claim.

Initial fact version

First relationship that seems stale or missing

The formation moves—or it fractures.

W/! CHANGE INJECTION

The webhook now invokes a serverless function through a workload identity and writes transaction references to a managed queue used by customer support.

Changed fact record

FIELD	WORKING RECORD
Changed subject and relationship	
Prior value	
New value	
Effective time	
Authoritative source	
Fact owner	
Known consumers	
Reopening trigger	

Every position has a different job.

01 Scope

Reopen the represented subjects and relationships. Which people, processes, technologies, locations, data flows, connected relationships, security-influencing relationships, and provider services require fresh analysis?

BOUNDED CLAIM	UNRESOLVED QUESTION

02 Applicability

Reopen predicates that depended on the prior facts. Which obligations, reporting responses, testing questions, or prior N/A conclusions relied on the old endpoint, identity, data path, or operating model?

BOUNDED CLAIM	UNRESOLVED QUESTION

03 Implementation and Responsibility

Name the operating verbs and accountable owners. Who configures, deploys, monitors, scans, tests, changes, responds, preserves, and proves the edge, function, identity, queue, provider handoff, and support use?

BOUNDED CLAIM	UNRESOLVED QUESTION

04 Evidence

Bound what can be supported now. Which objects support the correct subject, population, period, environment, and procedure—and where do staging evidence, stale targets, or absent propositions stop the claim?

BOUNDED CLAIM	UNRESOLVED QUESTION

Move. Reopen. Or hold with reason.

CONSUMER	QUESTION	MOVE / REOPEN / HOLD + REASON
System and component inventory	Does it identify the edge, function, workload identity, queue, and relevant environments?	
Software and application inventory	Does it identify the receiver code, dependencies, deployment source, and change owner?	
Architecture and data-flow narrative	Do the diagram and narrative agree about normal, failure, support, identity, and provider paths?	
Public-presence and scan target records	Have the actual terminating hostnames and infrastructure been reconciled to the applicable scan populations?	
Penetration-testing methodology	Does the method test the relevant external interface, trust transitions, identity, and application behavior?	
Provider assurance and responsibility	Do the exact service, callback behavior, customer configuration, and retained verbs reconcile to current assurance?	
Identity and access records	Is the workload identity attributable, bounded, reviewed, monitored, and linked to the correct deployment?	
SDLC and change record	Can the released function and configuration be traced from approved change through testing and production?	
Evidence contract and claims ledger	Do the evidence subject, environment, population, period, and provenance match the production claim?	
Assessment and reporting responses	Which prior assertions must reopen before the assessment can describe the current environment?	

Stop the conclusion where support ends.

EXPECTED	OBSERVED	ASSERTED	VALIDATED / NOT VALIDATED

Bounded disposition

SUPPORTED NOW	UNRESOLVED	ACCOUNTABLE OWNER	REOPENING TRIGGER

Assessor validation boundary

A reconstruction—not an answer key.

- 01 The changed fact is not merely a new URL; it is a new production relationship among an edge, receiver, workload identity, managed queue, provider callback, and support process.
- 02 The public interface and related infrastructure must be reconciled to the applicable external vulnerability, ASV, and penetration-testing populations; the exercise does not predetermine the result of that analysis.
- 03 Provider assurance must be reconciled to the exact service and callback behavior while retained customer verbs remain explicit.
- 04 The staging screenshot cannot, by itself, support a production implementation claim.
- 05 The assessment conclusion stops wherever the current subject, population, period, procedure, ownership, or evidence cannot be supported.

DEBRIEF

Which fact changed first? Which position looked current while another remained stale? Which provider and customer verbs needed separation? Which testing population or proposition required reconsideration? What could the evidence support—and where did support stop?

Preserve the first fracture.

FIELD	OBSERVATION
Session date	
Exact tested surface	
First missed dependency	
First oral rescue, or None	
Smallest repair	
Retest condition	
Workshop disposition	Repair and retest / Ready for second session / Hold
Known limitation	
NON-CLAIM This observation evaluates the workshop material. It is not an assessment result, scope conclusion, compliance result, or participant evaluation.	