

THE PROVIDER IS COMPLIANT. YOUR ARCHITECTURE STILL NEEDS AN EXPLANATION.

A service-provider assertion can support a responsibility claim. It cannot draw the customer's architecture, configure the service, or prove every customer duty occurred.

PRACTITIONER POSITION

Learners need to distinguish provider assurance from customer implementation. Study the exact service, assurance period, assessed scope, responsibility information, configuration assumptions, shared controls, customer duties, and change triggers. Do not turn a brand name or compliance statement into a universal scope conclusion. Provider reliance is strongest when the seam is explicit and testable.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A fictional startup uses hosted checkout and says the provider handles PCI. The startup still controls DNS, the merchant site, deployment, cloud identity, webhooks, API secrets, transaction metadata, refunds, logs, incident response, and provider configuration. The provider relationship reduces some exposure while creating a seam the team must explain.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The provider company is named but the exact service is not.
- An AOC is present without coverage and date analysis.
- Customer and shared duties have no owners.
- Configuration or feature changes do not reopen the responsibility map.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Identify the exact service, account, feature, region, integration, and environment.

Read assurance evidence for service coverage, period, limitations, and customer conditions.

Express responsibility in verbs such as configures, patches, monitors, tests, retains, investigates, and notifies.

Attach every deferral claim to customer proof and a change-monitoring owner.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Which exact service is covered?

02 What does the provider perform?

03 What remains with the customer?

04 Which change or assurance gap reopens the claim?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect service descriptions, assurance, responsibility, configuration, and data-flow facts.

02 / MAP

Assign provider, customer, or shared execution and evidence to each activity.

03 / EXPLAIN

State the narrow deferral claim and its limitations.

04 / REDUCE

Remove unused features and assumptions that widen the seam.

05 / PROVE

Retain current provider assurance and customer implementation evidence together.

THE FIELD LAW

THE LINE WORTH REMEMBERING

OUTSOURCING CAN REDUCE WORK. IT NEVER MAKES THE RESPONSIBILITY SEAM OPTIONAL.

Run the Provider Responsibility Interview against the fictional serverless startup.

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-0106 / Payment Card Industry Data Security Standard / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-15 against canonical digest

aa18321f659235a71aa401af98c086182c8e89d3e81c2e8078619672310f92ba. 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.