

EXPLAIN TPSP DEFERRAL AS A TESTABLE CLAIM

'We defer to the provider' is not an assessment result. It is the opening sentence of a claim that still needs a service, activity, boundary, evidence set, customer duty, test, and owner.

PRACTITIONER POSITION

My practitioner position is that every TPSP deferral should be expressed as a testable claim: for an exact provider service and configured use, identify the activity the provider performs, the environment and period covered, the provider evidence relied upon, the customer and shared duties still operated, the residual infrastructure and failure paths, and the monitoring and change triggers that keep the reliance current. 'Deferral claim' is practitioner method, not PCI SSC terminology. PCI DSS and PCI SSC FAQs govern the actual responsibilities and evidence expectations; the method helps an assessed entity explain them without turning a vendor name into a conclusion.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An assessed entity answers a requirement with 'covered by our cloud provider' and attaches an AOC. The AOC is current, but nobody has confirmed that its service scope matches the consumed service, that the cited requirement covers the relied-upon activity, that customer configuration duties are operating, or that a regional feature introduced during the year is included. The provider may be performing important work. The entity has not yet stated or supported the claim it wants the QSA to accept.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- A provider name, certification, AOC, or trust-center link appears where the assessed activity and responsibility should be described.
- The consumed product, feature, region, account, deployment model, version, or configuration cannot be reconciled to provider assessment scope.
- Responsibility is assigned only at the requirement level, hiding customer settings, shared handoffs, monitoring, evidence retention, and response duties.
- The entity cannot say which provider evidence supports which period, service, activity, and assessment result.
- No one owns annual provider-status monitoring, service-change review, AOC limitations, evidence requests, or a provider's failure to furnish sufficient evidence.

- The report language implies that responsibility was transferred even though customer-controlled infrastructure and operating duties remain.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI SSC FAQ 1312 explains that when a TPSP performs activities within or related to the customer CDE or can impact its security, the customer must manage and oversee the relationship, identify applicable responsibilities, and monitor the provider's compliance status. A requirement performed by a TPSP remains in scope of the customer's assessment; the provider's evidence affects the result.

PCI SSC FAQ 1576 expects a TPSP to provide evidence that its assessment scope covers the applicable services and relevant requirements. An AOC is one common form; when an AOC is unavailable, specific evidence may be needed. PCI SSC also points to a responsibility matrix as a useful way to communicate provider and customer duties.

A clear deferral claim reduces ambiguity without reducing accountability. It tells the QSA exactly what is asserted and gives the assessed entity an operating record for annual monitoring, service changes, provider evidence gaps, customer control failures, and report language. The claim is accepted or rejected through actual assessment work-not because its template is polished.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact service, feature, region, account, configuration, activity, population, and period does the reliance claim cover?
- 02 What does the provider perform, what does the customer perform, and what is shared at the level of actual control activity?
- 03 Does current provider evidence cover the consumed service and relevant requirements, and what limitation or carve-out changes the claim?
- 04 Which customer-controlled systems and people configure, authenticate to, integrate with, monitor, support, or respond to the service?
- 05 How will a service change, provider-evidence lapse, incident, control failure, or responsibility change reopen the claim?
- 06 Can the report state what was relied upon without implying that the provider assumed the entity's accountability?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

List each sentence in the assessment that says a provider performs, hosts, secures, validates, or handles something. Replace the vendor shorthand with the exact service, activity, environment, and period.

02 / MAP

Assign provider, customer, and shared performance at activity level; connect each assignment to provider scope, evidence, customer systems, owners, failure paths, and the assessment result it supports.

03 / EXPLAIN

Use the claim form: 'For [service/function], [TPSP] performs [activity] for [environment/population/period]; we rely on [current evidence], operate [customer/shared duties], and test and monitor [residual controls].'

04 / REDUCE

Remove unsupported reliance, unused provider features, ambiguous shared work, duplicate evidence requests, and report language that expands the provider's demonstrated coverage.

05 / PROVE

Retain the consumed-service inventory, responsibility matrix, current provider evidence, scope reconciliation, customer-control tests, limitations, monitoring record, change triggers, and exact report reference.

THE FIELD LAW

THE LINE WORTH REMEMBERING

DEFERRAL IS A CLAIM ABOUT PERFORMANCE AND EVIDENCE, NOT A TRANSFER OF ACCOUNTABILITY.

Take the assessment's broadest 'the provider handles it' statement and complete the one-sentence claim form. Every blank is either an evidence request, an owner assignment, or a limitation.

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-0023 / FAQ 1065: What is a TPSP expected to provide to customers as evidence of PCI DSS compliance? / PCI Security Standards Council / [Open source](#)

- WACK-SOURCE-0024 / FAQ 1576: What information are TPSPs expected to provide to customers? / 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

a09e49784b650d4bd9a90552fa544840b3f1fd4b82151b720784bcd5f482940c. 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.