

MAP TPSP RESPONSIBILITY WITHOUT THE HAND-WAVE

The provider logo belongs on the architecture diagram. "The vendor handles it" does not belong in the responsibility column.

PRACTITIONER POSITION

A useful TPSP responsibility map begins with the exact service consumed, then connects provider, customer, and shared activities to customer-side configuration, contractual commitments, validation coverage, evidence availability, exceptions, and ongoing monitoring.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A provider offers hosting, managed network controls, identity integration, logging, backup, and support. The contract names the product family. The current AOC covers several services. The customer configures accounts, rules, retention, and access. The assessment narrative assigns entire requirements to the provider because no one has decomposed the service into actual activities.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Responsibility is assigned at the requirement-family level without mapping specific activities.
- The service name in the architecture does not match the service coverage described in provider evidence.
- Customer configuration duties are absent from the responsibility record.
- Evidence expectations are discovered during the assessment instead of defined in advance.
- The annual TPSP review records status but not changes to services, coverage, or shared implementation.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI SSC guidance requires customers to manage and oversee TPSP relationships, identify which requirements apply to each party, and monitor TPSP compliance status. If a TPSP performs activities that meet requirements for the customer, the implementation and evidence for those services affect the customer's assessment.

The goal is not to force every service into a simplistic provider-or-customer box. Shared responsibility is common. The useful artifact makes the seam visible: who configures, who operates, who monitors, who

retains evidence, who handles failures, and what happens when service coverage changes.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 What exact provider service and deployment model is the customer using?

02 Which activities are provider-performed, customer-performed, or shared-and at what configuration boundary?

03 What evidence demonstrates each relied-upon activity, and when will it be available?

04 Who detects and resolves a gap when the contract, service, validation coverage, or implementation changes?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory every TPSP used within or related to the CDE and record the exact services and deployment models consumed.

02 / MAP

Decompose relied-upon controls into provider, customer, and shared activities, including customer-side configuration and evidence.

03 / EXPLAIN

Reconcile the responsibility map with contracts, service documentation, validation coverage, and current architecture.

04 / REDUCE

Close unmapped seams, remove unused services and permissions, and stop relying on evidence that does not cover the consumed service.

05 / PROVE

Maintain dated responsibility and evidence records, monitor TPSP status, and re-evaluate changes at least through the required review cycle.

THE LINE WORTH REMEMBERING

A PROVIDER CAN PERFORM THE ACTIVITY. THE RESPONSIBILITY SEAM STILL BELONGS ON THE MAP.

Which shared-responsibility seam will create your next evidence surprise?

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](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

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

fb942aa58bc03ec0082eb0c7664655a6e12c3ace333cde3272a5b164241641ee. 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.