

WACK CASE FILE / WACK-CONTENT-0062 / SEASON 1 FILE 03

THE VENDOR AOC THAT ANSWERED THE WRONG QUESTION

The document was current, authentic, and relevant to the provider. It still could not explain the customer's half of the service.

"The AOC was valid. The responsibility story was missing."

FICTIONAL COMPOSITE / REAL PRACTITIONER PATTERN

Fictional composite synthesized from common practitioner patterns. No client, assessment, or incident is described. Practitioner education, not PCI SSC terminology or a compliance determination. Independent resource; not affiliated with or endorsed by PCI SSC.

COLD OPEN

The vendor sent the AOC in eleven minutes. The team spent the next eleven weeks trying to make it answer a responsibility question it had never been designed to answer.

THE SCENE

The service provider was responsive, established, and central to the payment flow. Procurement had the contract. Security had the due-diligence packet. Compliance had a current attestation. The architecture diagram showed a neat cloud around the provider with one arrow entering and another leaving. Whenever responsibility came up, somebody pointed to the cloud and said the vendor handles that.

The sentence compressed several different ideas. The provider operated a service. The customer configured part of that service. An internal team decided which events entered it. Another team reviewed alerts. A separate group retained evidence. The AOC described the provider's assessed services and conclusions. It did not assign the customer's configuration, monitoring, escalation, or evidence duties for this particular implementation.

NARRATIVE TURN / 01

THE REQUEST THAT BOUNCED

A reviewer requested evidence for a monitoring activity. The internal owner sent the provider AOC. The reviewer asked where the customer responsibility was described. Compliance sent the contract. The contract named the service but not the operating control. Procurement sent the security exhibit. The exhibit promised capabilities but did not show who configured or reviewed them.

The request bounced among four teams because every document was real and none was the missing artifact. Each handoff widened Ownership Fog. People could identify who purchased the service, who administered it, who met with the vendor, and who received the bill. Nobody could point to one requirement-level or activity-level map showing the provider side, customer side, shared steps, and evidence source.

NARRATIVE TURN / 02

THE N/A SHORTCUT

Under deadline pressure, someone proposed marking the activity not applicable internally because the provider performed it. That conclusion felt efficient, but it repeated the original mistake. The question was not whether the provider did something related. The question was which exact activity the implementation required from each party and what facts supported that division.

The team opened the service documentation, contract, AOC, configuration screens, runbook, and alert queue together. The documents stopped competing once each was allowed to answer its own question. The AOC supported what had been assessed about the provider. The configuration showed what the customer enabled. The runbook showed who reviewed events. The queue showed how exceptions moved.

NARRATIVE TURN / 03

TURNING THE CLOUD INTO A SEAM

Instead of drawing one cloud labeled vendor, the team drew a seam. On the left: provider-operated platform activities and provider evidence. On the right: customer configuration, data selection, review, escalation, and retention. In the center: shared activities that failed if either side assumed the other had completed the handoff.

The responsibility map fit on two pages. It was less impressive than the AOC and more useful in the next meeting. Every row named the service activity, provider role, customer role, internal owner, evidence, and trigger for reassessment. The AOC remained important. It simply stopped being forced to impersonate a responsibility matrix.

WHAT THE TEAM FINALLY SAW

Wack by TPSP appears when evidence about a provider is treated as proof of the customer's complete operating model. The provider can be competent, the AOC can be valid, and the responsibility gap can still be wide open. The missing object is usually not another assurance document. It is a map of the specific service as implemented: who configures, who operates, who reviews, who responds, who retains evidence, and where the shared seams can fail.

THE WAY OUT

WORK THE METHOD.

01 / FIND

Collect the statements people use to transfer responsibility: the vendor handles it, it is covered by the AOC, or it is not applicable to us. Pair each statement with the exact service activity being discussed.

02 / MAP

For every activity, record provider responsibility, customer responsibility, shared steps, internal owner, evidence source, and unresolved question. Map the implemented service, not the vendor's marketing category.

03 / EXPLAIN

Let each document answer its proper question. Separate assessed provider services, contractual promises, technical capabilities, customer configuration, operating procedure, and actual evidence instead of blending them into one proof object.

04 / REDUCE

Eliminate ambiguous shared activities, duplicate reviewers, and undocumented handoffs. Where responsibility must remain shared, specify the event, artifact, or notification that proves the handoff occurred.

05 / PROVE

Keep the current responsibility map with the contract, provider assurance material, configuration evidence, operating records, and review trigger. Update it when the service, implementation, or provider scope changes.

FIELD NOTES

- An AOC is evidence about an assessed provider, not a customer responsibility matrix.
- The phrase vendor handles it should always be followed by which activity and which evidence.
- Shared responsibility needs a visible handoff, not a shared assumption.
- N/A is a conclusion supported by facts, not a deadline-management technique.

WHAT CHANGED

The evidence request closed after the internal team produced its configuration, review record, and escalation trail alongside the provider material. No heroic new control was invented. The team simply stopped asking one document to prove both sides of a relationship.

At the next vendor review, the first agenda item was no longer please send the latest AOC. It was show us what changed in the service, the responsibility seam, and the evidence path. The cloud on the diagram remained. Now it had edges, owners, and a door.

THE NEXT USEFUL QUESTION

TAKE THIS TO THE NEXT MEETING.

Choose one relied-upon provider service and map the provider, customer, and shared activities to named owners and evidence.

THREE LINES WORTH KEEPING

"The AOC was valid. The responsibility story was missing."

"Every document was real. None was the missing artifact."

"A provider cloud needs a visible seam."

FIND / MAP / EXPLAIN / REDUCE / PROVE

Fictional composite synthesized from common practitioner patterns. No client, assessment, or incident is described. Practitioner education, not PCI SSC terminology or a compliance determination. Independent resource; not affiliated with or endorsed by PCI SSC.