

AN AOC DOES NOT OUTSOURCE GOVERNANCE

Provider assurance matters. The customer still needs to understand the service, the allocation of responsibility, and the handoffs where assumptions accumulate.

By Scott Norton / PCI DSS QSA | Johanson Group, LLP

PRACTITIONER POSITION The vendor handles that is the beginning of a question, not the end of one.

A third-party service provider can perform important PCI DSS activities, operate technology, produce evidence, and maintain its own assessment. That can reduce operational burden and improve capability. It does not make the customer-provider relationship self-explanatory. The customer still needs to know which service is being consumed, how it is configured, which activities the provider performs, which remain with the customer, and what happens where the two responsibilities meet.

An Attestation of Compliance is valuable evidence about the provider and assessed services it describes. It is not a magic sentence that resolves every customer-specific responsibility. The document cannot know which service tier the customer purchased, which optional features are enabled, which customer configurations matter, who monitors the handoff, or how an exception moves from the provider into the customer's process.

OPERATIONAL RESPONSIBILITY CAN MOVE

Outsourcing changes who performs work. A provider may patch an underlying platform, manage physical access, operate a control plane, produce logs, or maintain infrastructure. The customer may rely on those activities. That is precisely why the allocation needs to be explicit. Reliance is an architectural and governance relationship, not a footnote attached after the scope conversation.

The mistake is not trusting a provider. The mistake is turning trust into vagueness. When the responsibility model is reduced to 'covered by the AOC,' the team loses the distinction between provider-performed, customer-performed, and shared activities. Shared does not mean both parties vaguely care. It means a handoff exists and each side needs to know the action, evidence, trigger, and escalation it owns.

START WITH THE CONSUMED SERVICE

Provider review should begin with the actual service relationship. Name the service and version or tier. Identify the components and features in use. Record where the service sits in the payment and security architecture. Then connect the provider's assurance documentation to that specific consumption pattern. A document about the provider is strongest when the customer can show why it applies to the service on the diagram.

This prevents a common form of Wack by TPSP: the provider has excellent documentation, the customer has a clean vendor inventory, and neither artifact explains the seam. The seam is where configuration choices, access paths, data flows, incident notification, evidence availability, and change communication cross organizational boundaries. That seam deserves an owner.

MAKE THE HANDOFF TESTABLE

For each relied-upon activity, ask five things: who performs it, what the other party must do, what evidence exists, how failure becomes visible, and who owns the next decision. This can live in a responsibility matrix, service register, control map, or another maintained source. The format matters less than the team's ability to retrieve a current and service-specific answer.

The evidence should follow the responsibility. Provider-performed activity may be supported by the provider's assurance material and service evidence. Customer configuration needs customer evidence. A shared handoff may need both. The goal is not to duplicate the provider's assessment. It is to make the customer's reliance and residual obligations understandable enough to operate and review.

GOVERNANCE IS THE CONNECTIVE TISSUE

Governance survives outsourcing because somebody must decide what is being relied upon, whether the evidence is relevant, how customer duties are assigned, and what happens when the service or assurance changes. Those decisions cannot be delegated into silence. They belong to the entity using the service, even when much of the technical operation belongs elsewhere.

A practical review does not begin by distrusting the AOC. It begins by respecting what the AOC actually answers and refusing to make it answer a different question. The provider may have demonstrated its environment. The customer must still demonstrate that it understands and governs the relationship it created by consuming the service.

FIVE QUESTIONS FOR THE NEXT WORKING SESSION

- Which exact service, tier, and features are we consuming?
- Which activities are provider, customer, and shared?
- What evidence supports each relied-upon activity?
- How does a failed handoff become visible and escalate?
- Who reviews the allocation when the service or assurance changes?

ONE MOVE TO MAKE NOW

Choose one critical provider service and map five relied-upon activities to the provider action, customer action, evidence, failure signal, and named decision owner.

THE PRACTITIONER POSITION

An AOC can answer an important assurance question. The responsibility model explains how that assurance connects to the customer's actual service, architecture, configuration, and operating obligations.

Operational responsibility can be delegated. Governance cannot disappear into the phrase 'the vendor handles that.'

AUTHORITY AND SOURCES

Independent practitioner perspective. Scott Norton is a PCI DSS QSA with Johanson Group, LLP. Unless specifically identified as an organizational position, the analysis and recommendations are his practitioner views, not formal positions of Johanson Group or PCI SSC. Cluster of Wack and related terms are not PCI SSC terminology. This material is educational and does not provide an assessment conclusion or imply endorsement by PCI SSC.

Authority classification: PRACTITIONER_POSITION / AI_ASSISTED. Authorship and authority classification do not determine legal intellectual-property ownership.

- PCI DSS v4.0.1 - PCI Security Standards Council: https://www.pcisecuritystandards.org/document_library/?class=pcidss&doc=pci_dss

- How is an entity's PCI DSS compliance impacted by using TPSPs? - PCI Security Standards Council: <https://www.pcisecuritystandards.org/faqs/1312/>