

YOUR QSA DOES NOT NEED THE PITCH DECK. THEY NEED THE ASSESSMENT FACTS.

PCI DSS transparency does not require a company to turn its ROC Executive Summary or AOC into a product architecture document, a competitive intelligence brief, or an attacker handbook.

PRACTITIONER POSITION

An assessment needs enough accurate, current, attributable detail for a qualified reviewer to evaluate the applicable PCI DSS claims. That does not mean every detail belongs in every artifact or with every audience. My practitioner position is that an assessed entity should manage disclosure by purpose: give the assessor the evidence needed to test the claim; give the ROC the detail required to document the assessment; give the AOC and customer assurance package a meaningful description of the assessed service, scope, account-data relationship, result, and responsibility boundary; keep unrelated product strategy, proprietary implementation, and unnecessary security-sensitive detail out of downstream documents. This is not secrecy as a scope strategy. It is precise information governance: disclose the PCI facts, preserve evaluability, and route each fact to the least-broad destination that can legitimately use it.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A payment startup prepares for its first ROC. Engineering supplies a pitch-deck diagram, a detailed internal architecture deck, and a list of product differentiators. The draft Executive Summary inherits all three. It names proprietary routing services, internal hostnames, cluster topology, security tooling, exact management paths, algorithm behavior, and roadmap capabilities. The customer-facing AOC then repeats much of the summary because the team assumes more detail is always more transparent. Legal proposes aggressive redaction; sales wants one universal assurance packet; engineering wants the whole architecture declared confidential; and the assessor still lacks a clean statement of the assessed service, payment channels, account-data behavior, security-impacting system categories, segmentation reliance, TPSPs, customer responsibilities, period, populations, and limitations. The company has disclosed the recipe while leaving the PCI claims hard to evaluate.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The Executive Summary was assembled by copying a product or architecture narrative instead of answering structured PCI reporting questions.

- The AOC names internal services, hostnames, IP ranges, management interfaces, clusters, algorithms, or security products that the recipient does not need to understand the validation.
- The same document is expected to serve the QSA, assessed entity, compliance-accepting entity, customer security team, sales team, legal counsel, and the public Internet.
- Confidentiality is used to withhold the subject, population, behavior, period, evidence, or limitation needed to evaluate a claim.
- Transparency is used to justify copying raw evidence and proprietary implementation detail into downstream reports.
- Redaction begins only after an over-detailed master document has already been circulated, duplicated, or uploaded to customer systems.
- Marketing language such as secure, compliant, industry-standard, or proprietary appears where the assessed service, account-data relationship, scope, result, or responsibility should be stated.
- Customers receive architecture detail but cannot determine which exact service was assessed, which responsibilities the provider performs, and which duties remain with them.
- Document metadata, filenames, comments, diagrams, screenshots, and appendices reveal information that the visible prose tried to minimize.
- No named owner can explain why a sensitive sentence appears in the ROC or AOC, which reporting purpose it serves, or what change should reopen the disclosure decision.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Start with the authority boundary. PCI SSC reporting templates, their instructions, applicable program rules, and compliance-accepting-entity direction govern what the validation artifact must contain. This manual is a practitioner information-governance method, not permission to omit required reporting or to replace an official form with a custom certificate. The destination decision begins only after the required reporting purpose is understood.

Separate the information planes. The evidence plane contains the detailed artifacts, observations, populations, configurations, interviews, tests, and limitations needed to evaluate a claim. The assessment-report plane communicates what was assessed, how testing supports the result, and why the recorded conclusion is bounded as written. The customer-assurance plane communicates the assessed service, scope, account-data relationship, applicable result, period, material provider and responsibility facts, and customer reliance conditions. A fact can be necessary in one plane and unnecessary in another.

Do not confuse information minimization with information denial. Proprietary or security-sensitive material cannot disappear merely because it is uncomfortable. If the detail is necessary to establish scope, applicability, control operation, testing coverage, a limitation, or an assessment conclusion, the assessor needs access through an appropriate controlled method. A protected review room, limited workpaper, redacted copy with the material facts intact, demonstration, or tightly held technical appendix can manage access. None of those mechanisms may make the claim impossible to evaluate.

Use the Council's AOC-sharing guidance carefully. PCI SSC FAQ 1354 says sensitive information may be redacted from an AOC when everything relevant to the purpose for which it is shared remains unredacted. It also identifies scope, covered services, requirements assessed, findings, and key attestation sections as relevant. That creates a disciplined test: the customer does not need every internal detail, but the resulting AOC must remain a meaningful summary of the assessed environment and, for a service provider, clearly identify the services covered.

Classify every candidate statement on three independent axes. First, PCI relevance: which scope, account-data, responsibility, control, testing, result, or reliance fact does it establish? Second, audience necessity: which recipient must use that fact and for what decision? Third, sensitivity: is it ordinary, confidential, proprietary, security-sensitive, regulated, or otherwise restricted? A high sensitivity label changes handling and abstraction. It does not answer relevance or necessity.

Climb the abstraction ladder without falling off it. Raw evidence may name exact services, identities, configurations, routes, data stores, and samples. A controlled architecture narrative may describe the relationships necessary to evaluate them. A ROC summary may state the payment function, data and influence paths, boundary, system categories, responsibilities, and testing result at the required level. An AOC may use a still-higher description suited to validation and reliance. The right level is the least specific statement that remains accurate, material, and sufficient for that artifact's purpose.

Describe function before recipe. 'The assessed payment platform routes transaction requests to downstream processors' may preserve the PCI-relevant function without publishing the proprietary logic that selects a route. 'The assessed service protects account data using tokenization' may be suitable for a customer-facing description while the assessor evaluates the implementation, cryptography, keys, data stores, failure paths, and evidence under controlled access. Abstraction is successful only when it removes irrelevant implementation detail without changing the claim.

Give customers responsibility clarity before architecture trivia. A service-provider customer usually needs to know whether the service stores, processes, transmits, or can impact payment account data; whether the exact service and relevant period were assessed; which activities the provider performs; which are shared; which remain with the customer; and what configurations or assumptions customer reliance requires. An AOC plus an exact-service description, current responsibility matrix, implementation responsibilities, and material limitations often answers those questions better than an architectural encyclopedia.

Author the customer-safe artifact natively. Drafting one reveal-all document and sanitizing copies afterward creates divergent versions, repeated legal review, forgotten comments, incomplete redactions, PDF-layer surprises, stale attachments, and a real chance that the wrong copy escapes. Start the AOC or assurance narrative at its intended abstraction. Link or reference controlled supporting material where the reporting instructions permit. Preserve one governed source for each statement and one explicit transformation record for every downstream representation.

Treat distribution as part of the control. Record the artifact, version, digest, audience, purpose, owner, approval, sensitivity, allowed destination, expiry or supersession rule, and withdrawal path. Customers upload AOCs into GRC platforms; sales teams attach them to tickets; procurement teams forward them; old copies remain in mailboxes. The useful drafting assumption is not that the document will remain secret. It is that every included fact should still be intentional if the artifact travels farther than expected.

Run both failure tests. The over-disclosure test asks what a competitor, attacker, or unauthorized recipient could learn that is unnecessary for the stated PCI purpose. The under-disclosure test asks whether a qualified reviewer or customer can still identify the assessed service, applicable scope and result, account-data and security-impact relationship, provider seams, responsibilities, limitations, and reliance conditions. Passing only one test produces either a dossier or a brochure. The goal is a bounded validation artifact.

Keep authorship, authority, and legal ownership separate. Engineering can own the technical facts, the assessed entity can make accountable representations, the assessor can evaluate evidence and record judgment, PCI SSC can remain the source of normative language and official reporting forms, and legal counsel can advise on confidentiality and intellectual-property handling. No single role should silently rewrite another role's claim. The final disclosure record should show who supplied, classified, abstracted, reviewed, approved, and distributed each material statement.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact reporting or reliance purpose does each sentence serve?
- 02 Which details must the assessor see to evaluate the claim, even if they should not appear in a customer-facing artifact?
- 03 Which service, scope, account-data, security-impact, responsibility, result, period, or limitation fact would disappear if the sentence were generalized?
- 04 Could the same PCI fact be stated accurately at a higher level of abstraction for this audience?
- 05 What proprietary terminology, implementation logic, internal identifier, topology, interface, or security detail is present without an audience need?
- 06 Would replacing architecture detail with an exact responsibility statement give the recipient more useful assurance?
- 07 Does any confidentiality or redaction choice make a claim unevaluable or an assessed service ambiguous?
- 08 Are hidden document layers, metadata, filenames, comments, diagrams, screenshots, links, or appendices governed by the same disclosure decision?
- 09 Which owner approves this exact version for this exact audience, and how is the approved digest recorded?
- 10 What architecture, service, provider, scope, result, responsibility, audience, or source change reopens the disclosure decision?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect the candidate statements, tables, diagrams, screenshots, appendices, metadata, and links from the evidence, ROC, AOC, responsibility, trust, sales, and customer-assurance artifacts. Identify the official reporting purpose and every intended audience.

02 / MAP

Join each fact to its claim, source, required destination, audience decision, sensitivity, owner, approved abstraction, supporting controlled evidence, version, digest, distribution path, and reopening trigger.

03 / EXPLAIN

Classify PCI relevance, audience necessity, and sensitivity independently. Write the least-specific statement that remains accurate, material, and sufficient, and document why any more detailed or more abstract version fails.

04 / REDUCE

Remove unrelated product strategy, proprietary recipes, unnecessary internal identifiers, attack-useful detail, duplicate narratives, and reveal-all masters while preserving required scope, service, responsibility, result, period, and limitation facts.

05 / PROVE

Run an assessor-read test, customer-reliance test, over-disclosure test, under-disclosure test, metadata inspection, and exact-version approval. Reopen the record whenever a material fact, source, audience, or distribution path changes.

THE FIELD LAW

THE LINE WORTH REMEMBERING

DETAIL HAS A DESTINATION. THE ASSESSOR GETS WHAT IS NEEDED TO EVALUATE THE CLAIM; THE CUSTOMER GETS WHAT IS NEEDED TO UNDERSTAND THE VALIDATION AND RESPONSIBILITY BOUNDARY; THE RECIPE STAYS CONTROLLED UNLESS THE CLAIM CANNOT BE TESTED WITHOUT IT.

Download the Minimum Necessary PCI Disclosure Matrix. Route one Executive Summary or AOC statement through PCI relevance, audience necessity, sensitivity, abstraction, evidence access, approval, and distribution before the document leaves the assessment team.

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-0008 / FAQ 1473: Role of compliance-accepting entities and assessors in determining applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0011 / FAQ 1382: Partial PCI DSS assessments documented in a ROC / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0013 / PCI SSC Document Library / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0080 / FAQ 1566: Can a QSA ask an auditor from the same company to collect evidence for a PCI DSS assessment? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0089 / FAQ 1354: Can sensitive information be redacted from the PCI DSS Attestation of Compliance before it is shared with other entities? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0090 / PCI SSC Releases ROC Template for PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / ASSESSOR_JUDGMENT / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-12 against canonical digest

ce81ebb8c3e0e92f43ad08e7021bcdff26142d13094fa69683f92dea45766869. 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.