

KEEP THE ACCEPTANCE BOUNDARY VISIBLE

The assessed entity and QSA can build and test a defensible position. They cannot silently make the compliance-accepting entity own a validation or reporting choice it did not accept.

PRACTITIONER POSITION

A defensible engagement distinguishes three related decisions: the compliance-accepting entity determines the required validation and reporting method; the assessed entity accurately represents its environment and the result it seeks to submit; and the assessor validates scope, applicability, testing, and reporting. When an approach would narrow what is tested, use SAQ eligibility criteria to guide a ROC, introduce Not Tested responses, or otherwise affect what the recipient is being asked to accept, the acceptance dependency must be explicit before the team presents the result as sufficient for that compliance program.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A merchant and its QSA agree that the environment resembles an SAQ-eligible channel and propose testing only that subset of requirements in a ROC. The technical rationale is thoughtful, the architecture is understood, and the proposed tests are clear. But the acquirer has not agreed that this reporting method or requirement set is acceptable. The assessment team is in danger of producing an accurate report that still does not satisfy the program to which it must be submitted.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The engagement letter names a ROC or SAQ but does not identify the entity that will accept the result or that entity's current reporting instructions.
- The assessed entity and QSA treat their agreement about an SAQ-derived requirement subset as sufficient without documented agreement from the compliance-accepting entity.
- Not Tested and Not Applicable are used interchangeably even though one excludes testing and the other requires the assessor to validate non-applicability.
- A partial assessment is described in conversation as if it were a complete PCI DSS compliance validation.
- An unusual applicability or reporting position depends on an unanswered acquirer or payment-brand question, but delivery proceeds as though silence were approval.

- The final report explains what was tested but not what the recipient was asked to accept, which instructions governed the submission, or which dependency remains unresolved.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI SSC FAQ 1473 separates responsibilities. Compliance-accepting entities determine validation and reporting methods and may direct which requirements are included. Assessors remain responsible for validating and documenting assessment scope and requirement applicability. A requirement reported Not Applicable must be confirmed through testing; a requirement not tested at all is reported Not Tested. Those are different statements to the report reader.

The current FAQ 1331 adds a specific boundary for merchant ROCs: SAQ eligibility criteria should not guide requirement applicability unless the approach is explicitly reviewed, discussed, and agreed with the merchant's compliance-accepting entity. FAQ 1382 permits a partial ROC but requires clear communication in both the ROC and AOC about what was and was not tested. FAQ 1142 routes compliance-program questions to the applicable payment brands or acquirer.

My practitioner position is that the assessed entity and QSA should not spend someone else's acceptance risk. That phrase is not PCI SSC terminology. It means the assessment team should identify the receiving party, surface any proposed departure from an ordinary full-validation path, present the facts and implications early, and preserve the recipient's direction. This does not outsource assessor judgment or let an acceptor relabel an applicable requirement as Not Applicable. It prevents a technically careful team from making a compliance-program acceptance decision on behalf of the organization that must bear it.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Who is the compliance-accepting entity for this result, and what current validation and reporting method has it required?
- 02 Which decisions belong to the acceptor, the assessed entity, and the assessor-and where is that responsibility split recorded?
- 03 Does the proposed approach use SAQ eligibility criteria to shape a ROC, exclude requirements from testing, or otherwise depend on recipient agreement?
- 04 For every Not Applicable response, what testing confirms that the requirement truly does not apply to the assessed environment?
- 05 For every Not Tested response, does the ROC and AOC make the partial nature and exact testing boundary unmistakable?
- 06 What unresolved question must be taken to the acquirer or payment brand before the result can be represented as sufficient for the compliance program?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Identify the intended compliance-accepting entity, its current program instructions, the proposed assessment and reporting method, every unusual applicability position, and every requirement proposed as Not Applicable or Not Tested.

02 / MAP

Create a decision map that separates acceptor direction, entity representation, assessor judgment, testing performed, reporting status, open dependencies, and the evidence supporting each one.

03 / EXPLAIN

Write the proposed position in recipient-readable language: what will be tested, what will not, why, which party owns each decision, and what the resulting ROC, SAQ, and AOC will and will not assert.

04 / REDUCE

Resolve acceptance dependencies before fieldwork becomes rework. Remove ambiguous shorthand, obtain current program direction, and avoid producing a full-report-shaped artifact for a partial or unaccepted validation path.

05 / PROVE

Retain the acceptor's direction, dated questions and responses, tested applicability rationales, Not Tested boundaries, report disclosures, and final submission requirements with the engagement record.

THE FIELD LAW

THE LINE WORTH REMEMBERING

OWN THE ANALYSIS. DO NOT SPEND THE ACCEPTOR'S RISK TOLERANCE WITHOUT THE ACCEPTOR.

Open the engagement plan and point to the compliance-accepting entity, its reporting instruction, and every decision that still depends on its agreement. If you cannot, the acceptance boundary is already foggy.

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-0008 / FAQ 1473: Role of compliance-accepting entities and assessors in determining applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0009 / FAQ 1331: SAQ eligibility criteria as a guide for ROC applicability / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0010 / FAQ 1142: How to contact the payment card brands / 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](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

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

8ae898cb00c709578eeef3829c979b664117798d94808df2f0aa0485e8a3e20d. 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.