

THE REQUIREMENT IS IN THE SAQ. THAT DOES NOT END THE APPLICABILITY QUESTION.

A row in a validation instrument tells you what must be answered. It does not, by itself, prove that the requirement's predicate is true in this environment-or that an unsupported N/A is acceptable.

PRACTITIONER POSITION

My practitioner position is that a Self-Assessment Questionnaire is a validation and reporting instrument, not an automatic applicability engine. The reasoning chain still has distinct gates: compliance-program direction, eligibility for the selected instrument, the assessed environment, the subject and conditional predicate of a requirement, observed architecture facts, evidence and testing, the recorded response, and the recipient's acceptance. Flatten those gates and two opposite errors appear. A team may treat every included row as universally applicable without asking whether its stated condition exists; or it may turn an eligibility statement into an automatic N/A without testing the environment. The useful discipline is not to make the questionnaire shorter. It is to preserve the logic that connects each answer to the exact subject, fact, condition, evidence, authority, and period that make the answer defensible. Requirement 1.4.4 inside SAQ A-EP is a revealing case study because the instrument's eligibility language and the requirement's storage-oriented condition can make a flat checklist look internally puzzling. The correct response is not to invent Council intent or erase the row. It is to verify current program direction and eligibility, identify the assessed subjects, evaluate the requirement predicate against observed facts, document the response and rationale, and reopen the instrument decision if the facts contradict eligibility.

WHAT THIS LOOKS LIKE IN PRACTICE

A merchant has been directed to complete SAQ A-EP. The team confirms the selected e-commerce integration but then reaches Requirement 1.4.4, which addresses direct access from untrusted networks to system components that store cardholder data. One group says the row must be In Place because it appears in the SAQ. Another says it must be N/A because A-EP eligibility includes no electronic storage, processing, or transmission of account data on merchant systems or premises. A third points at the assessor, while the assessor points back to the observed environment and the entity's representations. Nobody has recorded the actual system subjects, the account-data behavior tested, the requirement predicate, the evidence supporting the response, or what would happen if electronic storage were found. The questionnaire has become a proxy for reasoning. The hard question is not whether someone can imagine a control being present. It is what the requirement is asking about this assessed environment, why the selected response follows, and whether the answer exposes a contradiction that reopens eligibility or validation direction.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The team treats appearance in a questionnaire as proof that every factual condition inside the requirement is present.
- An eligibility criterion is copied into an N/A rationale without testing the current environment.
- A response says In Place but identifies no subject, control population, evidence, or testing result.
- A response says Not Applicable but identifies no predicate, observed fact, testing, limitation, or reviewer.
- The SAQ title is used to decide scope, applicability, or architecture facts that were never separately established.
- A contradictory fact-such as unexpected storage-is treated as a row-level exception rather than a trigger to reconsider eligibility and program direction.
- The assessed entity, assessor, and compliance-accepting entity are treated as one authority lane.
- Current PCI SSC instructions, SAQ version, completion guidance, and compliance-program requirements are not bound to the decision.
- A GRC platform offers only Applicable and N/A, with no place to record the requirement predicate or the evidence that evaluated it.
- The final answer survives only because the person who made it remains available to explain the missing logic verbally.

THE COST OF LEAVING IT UNEXPLAINED

Begin with program direction. PCI SSC states that compliance-accepting entities determine validation and reporting methods, including whether a ROC or SAQ is expected and whether a subset of requirements is to be tested. Confirm the current instrument, version, submission recipient, period, and any specific instructions. That direction defines the reporting lane; it does not manufacture the architecture facts used to answer it.

Establish eligibility before commencing the questionnaire. PCI SSC's October 2024 bulletin describes SAQs as validation tools for eligible entities, notes clarifications to A, A-EP, and C-VT, and tells merchants to confirm that all eligibility criteria are met before beginning. Eligibility therefore deserves its own record with each criterion, supporting fact, evidence, owner, date, uncertainty, and reopening trigger-not a single inherited yes/no field.

Keep eligibility, scope, applicability, and response separate. Eligibility asks whether the entity may use the instrument. Scope identifies the people, processes, technologies, locations, providers, and relationships considered. Requirement applicability asks whether the requirement or one of its stated conditions pertains to a defined subject. The response records what testing supports In Place, Not Applicable, Not Tested, or another permitted state. A conclusion in one layer cannot silently populate the next.

Read every requirement as a bounded proposition. Capture the requirement identifier and current wording reference, the subject class, the trigger or condition, the expected control state, the assessment procedure, and the response vocabulary allowed by the instrument. This is especially important for conditional language such as if, where, when, for systems that, or for entities that. Conditional does not mean optional; it means the predicate must be evaluated.

Use Requirement 1.4.4 in SAQ A-EP as a case-study question, not a shortcut. Confirm the current A-EP eligibility criteria and the actual merchant-side account-data behavior. Identify whether any assessed system component satisfies the storage-oriented predicate, including relevant memory and persistence behavior. If none does, preserve the tested basis for the response. If one does, treat the contradiction as a reason to reopen eligibility, scope, and recipient direction-not as permission to squeeze the fact into the originally selected form.

Distinguish an included question from a positive predicate. Instrument designers may include a requirement so an eligible population addresses, confirms, or documents it. The existence of the row establishes a response obligation within the selected instrument. It does not replace the environment-specific facts and testing needed for the response. Likewise, the absence of a requirement from a directed subset does not automatically prove that the requirement could never apply outside that validation decision.

Treat N/A as a tested proposition. FAQ 1473 says an assessor reporting a requirement Not Applicable must first confirm through testing that it truly is not applicable and document that confirmation. A useful N/A record names the subject and population, the predicate evaluated, the evidence and procedure, the observed result, the boundary and period, limitations, reviewer, and changes that would reopen the conclusion. 'The SAQ says so' and 'we do not do that' are not durable rationales.

Do not confuse Not Applicable with Not Tested. FAQ 1473 distinguishes a requirement tested and found not applicable from one excluded from testing. If the compliance-accepting entity directs an exclusion, preserve that direction and use the reporting treatment required by the current instrument and program. A hidden blank, filtered row, or unsupported N/A should never disguise an intentional exclusion.

Make contradictions first-class records. When an observed fact conflicts with an eligibility representation, scoped population, stated predicate result, or prior response, record the conflict, affected claims, immediate containment if necessary, decision owner, recipient question, and reopening status. The goal is not to protect the questionnaire choice. It is to protect the accuracy of the assessment story.

Design GRC tooling around predicates and lineage rather than rows alone. A useful model stores instrument version and direction, eligibility-criterion instances, architecture facts, scoped subjects, requirement predicates, evidence observations, test procedures, response decisions, authority, and temporal validity as linked objects. It can surface contradictions and missing joins without pretending to decide compliance. The user still owns the representation, the assessor still owns applicable independent evaluation, and the compliance-accepting entity still owns its program direction.

Escalate genuine interpretive questions without laundering them into local certainty. If the current SAQ, standard, instructions, FAQ corpus, and compliance-program direction do not resolve why a requirement is included or how a condition is intended to operate, state the precise question, the candidate interpretations, the consequence of each, and the current evidence. Seek direction from the appropriate authoritative or program party. Curiosity is not noncompliance; undocumented certainty is the dangerous part.

Close the chain with one reproducible decision packet. A cold reviewer should be able to see the instrument and version, program direction, eligibility basis, scoped subjects, requirement predicate, observed facts, evidence and test results, response and rationale, decision authority, limitations, effective period, recipient question, and reopening triggers. If those objects cannot be reconstructed without oral history, the answer is not yet assessment-ready.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Who directed the validation instrument, which version is current, and what exactly will the recipient accept?
- 02 What evidence supports every eligibility criterion before the first requirement response is entered?
- 03 What subject and population does this requirement address in the assessed environment?
- 04 What conditional predicate must be true before the control expectation becomes applicable to that subject?
- 05 Which observed architecture fact supports or contradicts that predicate?
- 06 What procedure tested the fact, and what evidence preserves the result and period?
- 07 Does the chosen response follow from the predicate evaluation, or from an assumption about the SAQ title?
- 08 Would a contradictory fact reopen only this response, or also eligibility, scope, validation direction, and earlier claims?
- 09 Are Not Applicable and Not Tested being kept visibly different in the record and final report?

10 Can a cold reviewer reproduce the answer without asking the author what the spreadsheet was supposed to mean?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect current compliance-program direction, instrument and version, every eligibility criterion, the assessed subjects, architecture facts, data behaviors, existing responses, and the exact conditions embedded in the relevant requirements.

02 / MAP

Join program direction to instrument eligibility, scope subjects, requirement predicates, observed facts, evidence, test procedures, responses, decision authorities, limitations, periods, recipient questions, and reopening triggers.

03 / EXPLAIN

Write each response as a bounded proposition: for this subject and population, during this period, this predicate was evaluated by this procedure against this evidence, producing this response with these limitations and authorities.

04 / REDUCE

Remove inherited answers, unsupported N/A rationales, silent exclusions, duplicate spreadsheets, and tooling fields that flatten eligibility, applicability, testing, and response into one status. Keep the smallest complete decision chain.

05 / PROVE

Run a contradiction drill. Introduce one fact that changes the predicate-such as newly discovered storage-and demonstrate that the response, affected eligibility claim, scope, recipient question, and dependent artifacts reopen together.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A ROW IN A VALIDATION INSTRUMENT IS AN ASSESSMENT QUESTION, NOT EVIDENCE THAT ITS PREDICATE IS TRUE.

Download the Applicability Predicate and Response Record. Trace one SAQ requirement from program direction through eligibility, subject, predicate, observed fact, evidence, testing, response, and reopening trigger-without asking a checkbox to do the reasoning.

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-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-0013 / PCI SSC Document Library / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0093 / PCI SSC Bulletin: SAQs for PCI DSS v4.0.1 Now Available / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0094 / FAQ 1291: Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0095 / FAQ 1293: SAQ A and A-EP payment-page eligibility / 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 2026-09-13 against canonical digest

cf532bf532cc5fcfb73d026957256c54af2575bca842a98e221750835043db37. 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.