

IN PLACE IS A CLAIM

Compliance labels are conclusions. The useful work is tracing each conclusion to the population, source, method, decision, and operating record beneath it.

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

PRACTITIONER POSITION Show me the source of truth.

'In Place' looks like a status. In practice it is a compressed claim about an environment, a control, a period, and a body of evidence. The same is true of 'Not Applicable,' 'outsourced,' 'segmented,' and 'out of scope.' Each phrase may be correct. None should be treated as the first fact in the analysis.

Evidence-before-assertion is not skepticism for its own sake. It is a discipline for unpacking the claim. What exactly is being asserted? For which systems, people, services, or processes? During what period? According to which source? Using what method? How were exceptions handled? Who owns the conclusion? Once those questions are answered, the status has a structure.

A SCREENSHOT IS NOT THE CLAIM

Evidence does not become persuasive because it is visual, recent, or exported from a trusted tool. A screenshot may accurately display a result while leaving the observed population, collection method, time boundary, exception state, and ownership invisible. The artifact and the claim are related, but they are not interchangeable.

The practical test is whether another person can move from the claim to the artifact and reconstruct why the artifact supports it. If the explanation depends on oral context, hidden filters, an undocumented query, or a population assembled separately, the evidence chain has missing links. More screenshots may create volume without repairing the chain.

READ THE TESTING PROCEDURE

The requirement states what must be achieved. The testing procedure gives essential clues about how an assessor will examine the claim: documents to review, people to interview, processes to observe, samples to select, configurations to inspect, or technical tests to perform. Stopping at the requirement can leave teams collecting the right topic in the wrong evidentiary shape.

This is not an invitation to design the control around passing a test. It is an invitation to use the testing procedure when designing the operating trace. If the assessment will need to understand a population, selection, observation, or configuration, the normal process should make that information maintainable rather than reconstructing it after the period ends.

SEPARATE SOURCE, TRANSFORMATION, AND CONCLUSION

Many evidence problems occur because a final report is treated as the source of truth when it is actually a transformation. An inventory feeds a query. The query produces a report. The report is filtered. The filtered result supports a reviewer decision. The decision becomes a status. Each step can be reasonable, but the chain needs enough lineage to explain what changed and why.

Name the authoritative source, the transformation logic, the resulting population, the reviewer action, the exceptions, and the final claim. This makes reuse safer. One artifact can support multiple claims when each use is explicit. Without lineage, reuse becomes Evidence Echo: the same file appears everywhere until nobody remembers what each copy was supposed to prove.

MAKE ONE STATUS EARN ITS LABEL

Pick one status that currently reads In Place, N/A, outsourced, segmented, or out of scope. Rewrite it as a complete sentence that names the subject, period, and condition. Then attach the source, population, method, exceptions, owner, and review trigger. The exercise is not complete when the folder contains a file. It is complete when the reasoning can be followed.

This changes review conversations. The team no longer debates whether an artifact 'counts.' It examines whether the chain supports the stated claim. Gaps become specific: missing population, stale source, unexplained transformation, unresolved exception, ambiguous owner, or unsupported conclusion. Specific gaps are easier to fix than generalized anxiety about evidence.

FIVE QUESTIONS FOR THE NEXT WORKING SESSION

- What exact claim is this artifact supporting?
- What is the authoritative source and complete population?
- Which transformation or filter produced the result?
- How are exceptions represented and decided?
- Who owns the conclusion and its next review?

ONE MOVE TO MAKE NOW

Take one green status and write the complete claim beneath it, including scope, period, population, source, method, exceptions, owner, and review trigger.

THE PRACTITIONER POSITION

Evidence quality is not a property of the file alone. It is the quality of the relationship between the file and the claim being tested.

In Place is a conclusion. Show the chain that allows another practitioner to reach it.

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
- Is sampling allowed in PCI DSS v4.x? - PCI Security Standards Council: <https://www.pcisecuritystandards.org/faqs/1569/>