LIVING ASSESSMENT READY

Readiness should be a living property of the operating model, not a temporary condition produced for an assessor.

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

PRACTITIONER POSITION The assessment should arrive to find the story already awake.

Assessment readiness is often described as a project with a kickoff, a tracker, evidence deadlines, escalation meetings, and a finish line. That model can produce a successful submission. It can also hide the fact that the program becomes legible only when assessment pressure supplies the missing coordination. A living assessment-ready program behaves differently: ordinary operations continuously preserve enough context to explain what is true, why it is true, who owns it, and what changed.

This is not a call to conduct a permanent mock assessment or keep every team in a year-round evidence sprint. It is a call to make readiness an output of normal work. The strongest program does not endlessly rehearse the assessment. It instruments important events, maintains accountable records, and can assemble the assessment story because the operating story never went dormant.

READINESS IS A PROPERTY, NOT A CALENDAR PHASE

A project plan can tell people when to upload evidence. It cannot make an inventory complete, a responsibility understood, or an exception current. Those conditions have to exist before the request arrives. Living readiness begins by naming the small number of operational states that must remain explainable: what is in scope, who performs each activity, which populations matter, how failure surfaces, and where decisions are retained.

The difference is visible in the questions teams ask. A seasonal program asks, ‘What does the assessor need this year?' A living program asks, ‘What happened since the last time this control was known to be healthy?' The first question organizes delivery. The second protects the truth of the environment. Both matter, but only one continues working after the evidence portal closes.

MAKE CHANGE PART OF THE ASSESSMENT STORY

Readiness decays when change and compliance live in separate systems. A new service, identity path, provider, network route, application version, or business process can alter scope and control expectations long before anyone updates the assessment workbook. A living model connects those events to the people and records that maintain the compliance story. Change does not merely modify technology; it creates a reason to revisit claims.

The useful trigger is not ‘update PCI documentation.' It is more precise: this change affected an asset relationship, introduced a new control performer, altered a tested population, or invalidated an earlier assumption. Those statements can drive targeted review without forcing the whole program back into assessment mode. Readiness becomes selective, event-aware, and proportionate.

KEEP CONCLUSIONS WARM WITH OPERATIONAL EXHAUST

Routine work already leaves traces: deployment records, identity events, configuration states, scan results, exception decisions, approvals, incident signals, and ownership changes. Those traces are not automatically assessment evidence. They become useful when the program knows the population, source, method, period, and conclusion each trace can support. Operational exhaust should reduce reconstruction, not become another pile of screenshots.

A living program therefore maintains evidence recipes rather than annual scavenger hunts. The recipe identifies where the source lives, which query or report is used, what completeness checks apply, who interprets the result, and what happens when the output is unexpected. The retained artifact matters, but the repeatable path to it matters more.

MEASURE WAKEFULNESS, NOT DOCUMENT VOLUME

Readiness metrics should reveal whether the program can notice and explain change. How many scope-affecting events reached compliance review? How many recurring controls completed on schedule? How long did exceptions remain without a current decision? How many evidence recipes failed because the source, owner, or population changed? These are operating questions. A count of uploaded files is mostly a logistics question.

The goal is not zero surprise. Real environments change, controls fail, and people learn. The goal is that surprise becomes visible through normal channels, reaches an accountable person, and leaves a decision trail. When that is true, the assessment can inspect the program rather than temporarily becoming the program.

FIVE QUESTIONS FOR THE NEXT WORKING SESSION

- Which assessment claim can become stale without any operational trigger noticing?
- What ordinary event should cause scope or evidence review?
- Which evidence package still depends on annual reconstruction?
- Who notices when an evidence source changes shape?
- What would remain understandable if the assessment moved forward by six months?

ONE MOVE TO MAKE NOW

Choose one recurring control and write its living readiness contract: trigger, population, source, owner, interpretation, exception path, retained record, and change condition.

THE PRACTITIONER POSITION

My practitioner position is that assessment readiness should be designed as a continuously explainable operating state. It should not require continuous panic, and it should not depend on a permanent assessor audience.

Let the assessment arrive. The architecture, ownership, evidence, and decisions should already be able to introduce themselves.

AUTHORITY AND SOURCES

Independent practitioner perspective. These dispatches are Scott Norton's practitioner analysis and recommendations, not PCI SSC terminology or guidance, not a formal position of Johanson Group, LLP, and not an assessment conclusion about any entity. AI assistance is recorded as production provenance; accountable professional judgment remains human.

Authority classification: PRACTITIONER_POSITION / PRACTITIONER_METHOD / 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