AUTOMATE THE MECHANICS. PRESERVE THE JUDGMENT.

Automation should give practitioners better context, cleaner populations, and earlier signals - not disguise an unsupported conclusion as machine certainty.

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

PRACTITIONER POSITION The tool should make the assessor better informed, not less responsible.

PCI DSS work contains enormous amounts of mechanical effort: collecting inventories, normalizing names, correlating assets, retrieving evidence, comparing periods, identifying changes, mapping records, and assembling work papers. Machines are well suited to much of that work. Refusing automation does not protect judgment. It often buries judgment under avoidable clerical effort.

The danger appears when automation moves from preparing context to manufacturing confidence. A tool can correlate the wrong population perfectly. It can summarize evidence whose lineage is weak. It can map a control based on an outdated relationship. It can produce polished prose that sounds more certain than the underlying facts. Automation can reduce Wack Tax, but it can also accelerate Wack Propagation.

AUTOMATE WHAT CAN BE REPRODUCED

Good automation begins with repeatable mechanical work. Retrieve the same source through a controlled interface. Normalize identifiers using declared rules. Compare current and prior populations. Flag missing relationships. Detect configuration changes. Assemble traceable evidence references. Generate a preliminary work paper that points back to the underlying artifacts. Each step should be reproducible and inspectable.

The test is not whether the automation uses AI. The test is whether another practitioner can understand the inputs, transformations, limitations, and output. Conventional scripts can be opaque. AI-assisted analysis can be transparent. Governance should follow the decision risk and the evidence chain rather than reacting only to the technology label.

RESERVE JUDGMENT FOR ACCOUNTABLE HUMANS

A machine can identify that evidence is missing, inconsistent, stale, or unusual. It can suggest a relationship or prepare a preliminary interpretation. It should not silently become the accountable party for scope, sampling, risk, control effectiveness, or compliance conclusions. Those decisions require context, challenge, professional responsibility, and an identifiable human owner.

Preserving judgment means designing explicit decision points. The system should show what it observed, what it inferred, how confident it is, and what it could not know. The reviewer should record the decision, rationale, exceptions, and follow-up. Automation becomes a force multiplier when it makes the human decision better informed and more traceable.

RISK-BASED NEEDS STRUCTURE

Automation often encounters the phrase ‘risk-based.' That phrase should trigger structure, not freedom from explanation. Where a frequency or action depends on risk, the analysis needs identifiable assets or processes, relevant threats, likelihood and impact considerations, the resulting decision, an approver, and a review condition. A generated score without that structure is just a faster opinion.

The same applies to sampling. A tool can help characterize a population and propose a selection, but the practitioner must understand why the sample is representative for the claim being tested. Automating selection does not outsource responsibility for the rationale. The machine can make the reasoning visible. It cannot be the reason.

INSTRUMENT THE COMPLIANCE ECOSYSTEM

The larger opportunity is to move from document-driven compliance toward an instrumented compliance ecosystem. Maintained asset inventories, identities, configurations, service relationships, evidence records, changes, and ownership can provide the context from which many assessment artifacts are derived. The GRC platform becomes a repository of connected sources of truth instead of the place where annual answers are pasted.

Start with one workflow where people repeatedly reconcile the same facts. Preserve the authoritative sources. Automate retrieval and normalization. Expose discrepancies rather than smoothing them away. Insert a named human decision. Retain the lineage from source to conclusion. That pattern reduces mechanical effort while increasing accountability - the combination that makes automation worth trusting.

FIVE QUESTIONS FOR THE NEXT WORKING SESSION

- Which mechanical step is repeated and reproducible?
- What are the authoritative inputs and declared transformations?
- Where does inference begin and what can the system not know?
- Which human owns the resulting decision?
- Can a reviewer trace the conclusion back to the source records?

ONE MOVE TO MAKE NOW

Choose one repeated evidence-reconciliation workflow and automate retrieval, normalization, and change detection while preserving an explicit human decision and complete lineage.

THE PRACTITIONER POSITION

The goal is not human judgment surrounded by manual drudgery. It is human judgment supplied with better context, cleaner populations, earlier discrepancies, and a traceable record of how the decision was reached.

Automate the mechanics aggressively. Preserve the judgment deliberately.

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/