

THE QUARTERLY SCAN YOU DID NOT KNOW YOU NEEDED

A missed external scan is often discovered during the annual form because nobody translated program direction into owned recurring work.

PRACTITIONER POSITION

A merchant should not infer ASV applicability from this article, a website pattern, or an old questionnaire. It should obtain current validation direction, identify the applicable Internet-facing population, engage an approved scanning vendor where required, understand the passing and remediation process, retain results, and put the occurrence on an operating calendar. A late scan can show a later state. It does not recreate a missed earlier occurrence. The useful response is prompt escalation, accurate chronology, corrective action, and prevention-not a rewritten date.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

An ecommerce member opens its annual compliance portal and learns that quarterly ASV scans were expected. The website redirects customers to a provider, so the owner assumed scanning belonged entirely to the host or processor. There is no documented target population, scanning-vendor relationship, calendar owner, quarterly result set, or escalation path.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Scanning is discussed only when the annual questionnaire opens.
- The target list is copied from a prior period without current website and DNS reconciliation.
- A hosting or payment provider is assumed to perform the merchant's required scan without evidence.
- A late passing result is presented as if it proves an earlier quarter occurred.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Ask the compliance-accepting entity which validation activities apply to the current merchant environment and which official documents govern them. Preserve the response and date.

Where ASV scanning applies, identify the merchant webpages and public infrastructure relevant to the required population, the ASV, the scan account, the owner, the target source, and the expected result-handling process.

Treat every occurrence as a dated operating event. Retain target population, submitted scan, result, remediation, rescan, exception handling, and the decision trail for additions or exclusions.

If an occurrence is missed, contact the accepting entity rather than inventing a cure. Complete current work, preserve the missed chronology, address causes, and prevent recurrence.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

01 Who told the merchant which external scanning obligations apply?

02 Which public systems or webpages belong in the applicable target population?

03 Who owns each occurrence, result, remediation, and rescan?

04 What will the merchant do immediately if the next occurrence is late or fails?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect current program direction, website and public-presence inventories, prior scans, ASV account information, and missed occurrences.

02 / MAP

Connect every applicable target and quarter to an owner, ASV submission, result, remediation, rescan, evidence location, and escalation path.

03 / EXPLAIN

Distinguish current scanning evidence, historical occurrence evidence, corrective work, and accepting-entity treatment.

04 / REDUCE

Remove stale targets and ownership gaps while preserving evidence for every current inclusion, separate coverage, or fact-specific exclusion.

05 / PROVE

Show the current population, each required occurrence, passing evidence where applicable, remediation lineage, and the recurrence control.

THE LINE WORTH REMEMBERING

A SCAN PERFORMED TODAY CAN DESCRIBE TODAY. IT CANNOT TRAVEL BACKWARD AND BECOME LAST QUARTER.

Put the next expected activity, owner, evidence, and escalation contact into the Recurring Work Planner before closing the annual portal.

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-0006 / Resource Guide: Vulnerability Scans and Approved Scanning Vendors / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0033 / FAQ 1087: Quarterly vulnerability scanning timeframes / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0062 / FAQ 1152: Requirement to complete four passing quarterly ASV scans / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0102 / FAQ 1604: ASV scans for SAQ A redirect and embedded-payment-page merchants / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-15 against canonical digest 18655b4d44db0d236fdb7cdf17f0db548cc74bf5abbab1420ef29fff9e76fe1. 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.