

DISCLOSE THE RELEVANT PUBLIC EDGE BEFORE YOU DEFINE THE ASV SCOPE

Do not begin an ASV conversation with the addresses you hope are in scope. Begin with the known public points of presence that are in the CDE, connect to it, or could impact its security-and keep unresolved candidates visible until their relationship is decided.

PRACTITIONER POSITION

A strong ASV scoping process discloses the known public attack surface that is within the CDE, connected to the CDE, or capable of impacting the security of the CDE, plus unresolved candidates whose relationship has not yet been established. It then classifies each relevant address, range, domain, hostname, application entry point, cloud endpoint, and provider-hosted presence as included, separately covered, or excluded with a documented rationale, evidence, owner, and change trigger. Disclosure is the practitioner method; the applicable PCI DSS and ASV scan scope remains a fact-specific determination.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

The quarterly ASV request contains the same four IP addresses as last quarter. DNS now resolves the payment site through a content-delivery service, a new cloud load balancer hosts an administrative path, a disaster-recovery endpoint is publicly reachable but idle, and a marketing domain redirects into the payment journey. Security knows about some of these endpoints. Infrastructure knows about others. The ASV sees only the submitted list, while the scope spreadsheet labels the rest out of scope without preserving who made that decision or what evidence supports it.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The ASV target list is copied from the prior quarter without reconciliation to current DNS, cloud, certificate, CDN, hosting, and external-attack-surface sources.
- Public endpoints with a known or plausible CDE relationship disappear from the disclosure package after being marked out of scope instead of remaining visible with rationale and accountable approval.
- Domains, hostnames, URLs, IPv4 and IPv6 addresses, cloud endpoints, provider-hosted paths, and alternate entry points are maintained in separate owner-specific lists.
- The organization cannot distinguish an endpoint excluded by a documented scope decision from one omitted because no team knew it existed.

- A third party, shared host, CDN, or redirect is treated as invisible rather than mapped to the service, responsibility, evidence, and scan-coverage arrangement.
- Discovery differences found by the ASV or another external source are closed in the scan portal but never routed back to inventory, diagrams, or scope governance.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

PCI DSS Requirement 11.3.2 addresses external vulnerability scans performed by a PCI SSC Approved Scanning Vendor at least once every three months, with applicability depending on the entity and validation context. PCI SSC's ASV resources explain the role of ASV scans and, for SAQ A e-commerce merchants, the focus on systems hosting webpages that redirect to or embed third-party payment pages. Those authoritative sources should control the compliance statement; neither a practitioner slogan nor an inventory convention should be presented as an additional PCI DSS requirement.

My practitioner position is intentionally broad at the PCI-relevant discovery boundary, not across every unrelated corporate endpoint: disclose the known public edge that is in the CDE, connected to it, or capable of impacting its security, and keep uncertain candidates visible until their relationship is resolved. That disclosure does not mean every endpoint is necessarily in PCI DSS scope or must appear on the same passing scan. It means the relevant population is visible to accountable participants, and every non-included endpoint carries a reviewable explanation instead of vanishing before the scoping conversation begins.

This approach protects against omission masquerading as exclusion. It also improves operational security because the entity can compare PCI-relevant ASV coverage with broader external attack-surface management without confusing their purposes or reports. The useful record preserves what was disclosed, what the ASV scanned, what another party covered, what was excluded, why, who decided, which evidence supports the decision, and what change would reopen it.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What is the known population of public IP addresses, IPv6 addresses, ranges, domains, hostnames, URLs, application entry points, cloud endpoints, and provider-hosted presences that are in the CDE, connect to it, or could impact its security?
- 02 Which independent sources-DNS, certificates, cloud inventories, load balancers, CDNs, hosting records, attack-surface discovery, and prior scan results-were reconciled to find omissions?
- 03 For every public point of presence, is it included in this ASV scan, evidenced as separately covered, or excluded through a documented fact-specific scope decision?
- 04 What architecture, data flow, administrative path, security impact, redirect, embedded component, or provider relationship supports each classification?
- 05 Who owns the endpoint and the classification, when was it verified, and which change event forces reconsideration?

06 How are ASV discoveries and target-list differences returned to inventory, diagrams, scope governance, and the next scanning cycle?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Assemble the broadest defensible inventory of public presences with a known or plausible CDE relationship from organizational records and independent discovery sources before filtering for PCI DSS or ASV applicability.

02 / MAP

Connect each public point of presence to its service, system, owner, payment or administrative path, provider, data flow, scope classification, and scan-coverage status.

03 / EXPLAIN

Record one of three transparent dispositions for every endpoint: included in the ASV scan, separately covered with evidence, or excluded with rationale, evidence, decision owner, review date, and change trigger.

04 / REDUCE

Remove abandoned public exposure, consolidate duplicate entry points, correct misleading DNS and ownership records, and eliminate unsourced exclusions that cannot survive review.

05 / PROVE

Retain the CDE-relevant population snapshot, unresolved candidates, ASV-submitted population, reconciliation sources, classification decisions, discovered differences, passing evidence where applicable, and remediation or rescan lineage.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A RELEVANT ENDPOINT CAN SURVIVE AN OUT-OF-SCOPE CONCLUSION. AN OMITTED ENDPOINT NEVER RECEIVED ONE.

Ask for the CDE-relevant public-edge population-not only the current ASV list. Which endpoint is absent because its relationship was analyzed, and which is absent because nobody asked?

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](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-09 against canonical digest

a53bb79b0ade0ef0b3bbaf9f6e983e7e6fcd059112f1a1802330e1e82e8060a4. 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.