THRIVEPCI / FIELD GUIDE

Six Zones, Four Boundaries

A practical method for diagrams, registers, and testable questions

PCI DSS v4.0.1 | Learner edition | Draft 0.1.0

What you will do

Use a fictional payment environment to identify scope questions, trace an account-data flow, record an allowed connection, and define one denied-path test question. The goal is a set of artifacts that agree and can be reviewed.

Important boundary

The six-zone model is an independent practitioner teaching aid, not PCI SSC terminology. It does not determine scope, compliance, validation eligibility, or assessment outcome. Use PCI DSS v4.0.1, applicable program instructions, and qualified review for those decisions.

1. Begin with system function

A network label does not settle scope. Ask what each component stores, processes, or transmits; what can connect to it; and whether it can affect the security of the cardholder data environment (CDE). Record facts separately from assumptions and conclusions.

Question	Record
What does the component do?	Business and technical function; owner; environment
Does it handle account data?	Data elements, direction, storage, processing, transmission
What can it reach or influence?	Connections, trust relationships, management and control paths
What evidence supports the answer?	Current diagrams, configuration, interviews, tests, provider records
Who confirms the scope decision?	Entity owner and assessor, using applicable PCI DSS language

The six labels used in this course

Model zone	Example focus	Teaching prompt
Z0 · untrusted	Internet, carriers, third parties	Where does untrusted traffic enter?
Z1 · edge	Public-facing and access services	Does a component handle or transmit account data?
Z2 · CDE (Z2a / Z2b)	Application and data examples	Where does data enter, and which systems store it?
Z3 · shared services	Identity, logging, time, scanning, backup	Could this service affect CDE security?
Z4 · privileged access	Administrator workstations and access tools	Where are access controls applied?
Z5 · corporate	General user and development environments	What evidence demonstrates claimed isolation?

These are model labels, not PCI DSS categories. Zone assignment must follow the component's real function, relationships, and the standard's scope rules.

2. Draw connections before drawing conclusions

Start with one payment. Draw the path from cardholder entry through the payment service and onward to the processor. Add supporting services and administrator connections. A network diagram and an account-data-flow diagram answer related but different questions; keep both current and reconcile them.

Four named boundaries in this teaching model

Label	Model role	What to examine
NSC-1	Perimeter	Authorized inbound services, responses, external exposure
NSC-2	Internal CDE boundary	Connections into and out of CDE components
NSC-3	Claimed scope separation	Paths that could invalidate an out-of-scope claim
NSC-2a	Nested sub-boundary within NSC-2	Illustrative separation between application and data zones

NSC-2a explains the source set's boundary-count ambiguity. Here it is a nested sub-boundary, not an additional peer boundary. Actual environments may use other logical designs and counts.

Flow register starter

ID	Source → destination	Service / direction	Business reason / owner
F-01	Cardholder → public edge	HTTPS / inbound	Payment acceptance · owner: _____
F-02	Payment service → processor	Actual service / outbound	Authorization and settlement · owner: _____
F-03	CDE → logging service	Actual service / outbound	Security monitoring · owner: _____

Use actual ports, protocols, endpoints, owners, approvals, and review evidence. The examples are prompts, not required architectures. Requirement 1.2.5 and other applicable requirements govern what must be documented.

3. Turn isolation claims into test questions

List each path that should not exist. Define the source, destination, boundary, expected result, and evidence. Determine the applicable segmentation-testing requirements and timing from PCI DSS and the entity's status. A register can organize tests; it cannot substitute for the required method or conclusion.

ID	Path to test	Expected result	Evidence / owner
D-01	Corporate workstation → CDE host	Blocked / no effective route	Test record: _____
D-02	Guest Wi-Fi → CDE services	Blocked as applicable	Test record: _____
D-03	Untrusted network → stored-data system	Not directly reachable as applicable	Test record: _____

Keep the identifiers controlled

The supplied source deck uses inconsistent deny references in places. Before a reviewer relies on a package, reconcile each ID across the diagram, register, test procedure, and result. Do not infer which identifier was intended.

Cross-check the evidence set

- Network diagram ↔ inventory and network security control configuration
- Account-data-flow diagram ↔ flow register and processor/provider relationships
- Boundary claims ↔ test method, results, and relevant exceptions
- Scope confirmation ↔ current systems, locations, services, and changes

Practice scenario

Lumen Learning accepts card payments on a public site. A payment service sends transactions to a processor. A shared identity service, logging platform, patch repository, and backup service support the payment environment. Corporate staff use separate laptops and Wi-Fi. The diagram shows no direct corporate route to the CDE, but a corporate administrator can manage the shared identity service.

Discuss: Which facts are still missing? Which shared services require scope analysis? What route or trust relationship needs investigation? What would you record as an allowed flow? What evidence would support the claimed corporate separation? Do not decide scope from the scenario alone.

4. Debrief and source map

Statement	Classification
PCI DSS defines scope and applicable testing requirements.	Standard requirement / guidance; verify exact wording and applicability.
The six zones organize a discussion.	Independent teaching model.
Tokenize at the first CDE hop.	Illustrative design recommendation in the source model.
A shared service is in scope.	Evaluate its capability and relationship under the standard; do not infer from the label alone.
A deny register uses IDs that match tests.	Practitioner recordkeeping method supporting traceability.

Suggested source review

PCI DSS v4.0.1, June 2024: Scope of PCI DSS Requirements; Requirement 1 overview and Requirements 1.2.3 –1.2.7, 1.3, and 1.4; Requirements 8.4.2–8.4.3; Requirements 11.4.5–11.4.6; Requirement 12.5.2 and related applicability. Check the specific requirement, testing procedure, notes, and current program documents before relying on a citation.

Review and recording status

This is a draft for Scott’s technical, editorial, accessibility, and rights review. The editable trainer presentation contains owner-recorded narration copy in speaker notes. No audio or video has been recorded. After recording, return the MP4 for caption, playback, accessibility, and publication review.

Source lineage: TCOW-PCI-ZONE-RA-001 v1.5; TCOW-PCI-ZONE-GDE-001 v1.2; TCOW-PCI-ZONE-TRN-001 v1.2. The source set identifies its framework as a practitioner model and not a PCI SSC publication. This ThrivePCI adaptation does not reproduce its figures.

Current standard and assessment timing

The phase-in has elapsed

Requirements and specified bullets previously phased in on March 31, 2025 are effective. Apply their entity, technology and other applicability conditions.

Use the current successors

6.4.1 6.4.2 | 8.3.10 8.3.10.1 | 10.7.1 10.7.2. The superseded requirements are N/A for current reporting; retain them only for historical context.

Keep timing and evidence distinct

An effective date does not create a recurring control interval or an evidence freshness limit. Use the applicable requirement and testing procedures to establish those obligations.

Source: PCI DSS v4.0.1; PCI SSC FAQs 1593 and 1176. Source checked November 21, 2026.

PCI DSS v4.0.1 / corpus 1.1.0+20261121T170000Z