thrivePCI

COURSE 07

Six Zones, Four Boundaries

A practical method for diagrams, registers, and testable questions



Trainer edition 0.1.5+20261120T222000Z · Draft for Scott review

The outcome is a set of agreeing artifacts

01 **Network diagram: components, connections, and controls**

02 Account data-flow diagram: each account-data path

03 Registers and tests: why flows exist and whether denied paths stay closed

DRAFT FOR REVIEW

Start with the scope categories

01

CDE: stores, processes, or transmits account data

02

Connected-to or security-impacting systems may also be in scope

03

Out-of-scope claims depend on demonstrated isolation and impact

DRAFT FOR REVIEW

The six zones are a teaching map

01

Z0

untrusted networks and third parties

02

Z1

edge services; classification depends on function

03

Z2a / Z2b

CDE application and data examples

04

Z3

security and shared services

05

Z4

privileged access systems

06

Z5

corporate systems claimed as out of scope

DRAFT FOR REVIEW

Four boundaries, with one explicit sub-boundary

01	**NSC-1**	perimeter
02	**NSC-2**	internal CDE boundary
03	**NSC-3**	claimed scope separation
04	**NSC-2a**	illustrative intra-CDE separation within NSC-2

DRAFT FOR REVIEW

Trace one payment from browser to processor

01 **Cardholder → public edge → payment application**

02 Identify every account-data touchpoint

03 Show the processor path and named destinations

04 Record each allowed connection and its business purpose

DRAFT FOR REVIEW

Separate shared services from ‘non-CDE’ labels

01 **Identity, logging, time, name resolution**

02 Scanning, malware and change-detection consoles

03 Backup, patching, and deployment tooling

04 Assess each service’s ability to impact CDE security

DRAFT FOR REVIEW

Make the administrator path visible

01 **Identify remote access entry points**

02 Show privileged access management and target systems

03 Record where authentication controls apply

04 Avoid inferring one universal architecture from the example

DRAFT FOR REVIEW

A scope boundary is a claim to prove

01 **List the systems proposed as out of scope**

02 Identify every path that could affect the CDE

03 Test the relevant segmentation controls

04 Record the evidence and any exceptions

DRAFT FOR REVIEW

Allowed flows need useful records

01 **Source and destination**

02 Service, port, and direction

03 Business purpose and owner

04 Approval and review evidence where applicable

DRAFT FOR REVIEW

Deny paths need precise test cases

01

Name the source and target

02

Define the boundary and expected result

03

Capture how the test was performed

04

Resolve inconsistent identifiers before review

DRAFT FOR REVIEW

Variants change the questions, not the method

01 **Cloud: include control-plane and service relationships**

02 Multi-tenant: assess tenant separation and Appendix A1 applicability

03 Merchant: examine the payment page and integration model

04 Confirm the reporting path with the applicable program

DRAFT FOR REVIEW

Use the model as a cross-check

01

Network diagram ↔ system inventory

02

Data-flow diagram ↔ flow register

03

Boundary rules ↔ segmentation test evidence

04

Scope confirmation ↔ current environment

DRAFT FOR REVIEW

Take one concrete next step

01 **Choose one payment flow**

02 Map its real systems and account-data touches

03 Record one allowed path and one denied path

04 Ask the assessor or program owner about unresolved applicability

DRAFT FOR REVIEW

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