thrivePCI

COURSE 04

Provider Responsibilities

Your providers and your retained work



Release 0.1.7+20 261 120T222 000Z | Draft for review

Learning objectives

01

Identify the service actually consumed

02

Correlate provider coverage and responsibility information

03

Record retained work and unresolved questions

DRAFT FOR REVIEW

The consumed service

01

Provider name and service coverage are different facts

02

The deployed arrangement needs a current description

03

Responsibility analysis starts with the actual service

DRAFT FOR REVIEW

A provider evidence packet

Each document answers a different question
Coverage needs correlation to the consumed service

Record	Question it helps address
Consumed service description	What service and environment do we use?
Appropriate AOC or supporting status record	What assessed coverage and status are represented?
Responsibility information	Which activities are provider, customer or shared?
Relevant agreement and acknowledgment	What responsibilities does the arrangement acknowledge?

DRAFT FOR REVIEW

Provider, customer and shared work

01

12.8.5 calls for responsibility information

02

12.9.2 is an additional requirement for service providers

03

Customers retain and evidence their assigned work

DRAFT FOR REVIEW

An illustrative responsibility row

Provider coverage needs a precise reference
Shared activities need both sides explained

Mapping field	Illustrative content
Service and relevant activity	Managed service and identified operation
Provider responsibility reference	Provider document, section and version
Retained customer activity	Customer setting and retained review
Customer evidence reference	Approved configuration and activity records

DRAFT FOR REVIEW

Provider oversight over time

01

Due diligence precedes engagement

02

Status monitoring has an explicit minimum frequency

03

Changes and gaps need follow-up

DRAFT FOR REVIEW

A specific provider question

Name the consumed service and relevant activity
Request the missing coverage or responsibility detail

Question component	Illustrative request detail
Service	The named managed service we consume
Activity	The specific responsibility needing clarification
Reference	Current document section and version
Requested output	Party allocation, coverage and retained customer work

DRAFT FOR REVIEW

Practice scenario

01

An AOC names a provider’s hosting service

02

The customer also buys an optional managed service

03

The responsibility document does not mention that option

DRAFT FOR REVIEW

Scenario debrief

The optional service needs its own correlation
Retained work remains explicit while the question is open

Open item	Preparation owner and next output
Optional service description	Vendor owner: service-specific information
Deployed configuration	Technical owner: actual arrangement
Provider/customer division	Vendor and readiness owners: correlated mapping
Unresolved reliance claim	Program owner: visible gap and follow-up

DRAFT FOR REVIEW

Knowledge check

Which statement is supported?

A. One provider AOC covers every product by default

B. A provider removes all customer duties

C. The consumed service and responsibility information need correlation

D. Shared work means neither party retains evidence

DRAFT FOR REVIEW

Answer and explanation

01

C is the supported answer

02

Responsibility follows the service and actual activity division

DRAFT FOR REVIEW

Your provider action brief

01

Choose one consumed service

02

Correlate coverage, responsibilities and retained evidence

03

Assign unanswered questions to the vendor owner

DRAFT FOR REVIEW

Sources and course boundary

PCI DSS v4.0.1: third-party provider management

12.8.5: requirements managed by each party or shared

12.9.2: service-provider support for customer requests

Educational guidance. No compliance guarantee.

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