thrivePCI

COURSE 06

# Sustaining the Program

The work between assessments



Release 0.1.6+20 261 120T210 500Z | Draft for review

# Learning objectives

**01**

Separate program planning from required frequencies

**02**

Identify changes needing responsible review

**03**

Prepare an owner and knowledge handover



DRAFT FOR REVIEW

# Business-as-usual program work

**01**

Control operation continues between assessments

**02**

Monitoring and follow-up keep changed facts visible

**03**

Specific requirements still govern each activity



DRAFT FOR REVIEW

# Three types of timing information

Required frequencies need an authoritative basis
Internal planning dates support coordination

| Timing category | Basis to retain |
| --- | --- |
| Explicit standard frequency | Applicable requirement and exact timing |
| Permitted risk-based frequency | Applicable requirement and documented TRA |
| Internal planning date | Owner’s coordination decision |
| Review after relevant change | Applicable trigger and actual changed facts |



DRAFT FOR REVIEW

# Relevant changes need review

**01**

Payment processes and provider services can change

**02**

Owners and system arrangements can change

**03**

The responsible parties need current facts



DRAFT FOR REVIEW

# A change review conversation

Describe what changed and the affected service
Record the responsible review and follow-up

| Conversation field | Useful factual input |
| --- | --- |
| Changed arrangement | Previous and current service or process |
| Affected records | Scope, provider and operating documentation |
| Responsible review | Named authorized business and technical owners |
| Follow-up | Documented actions, evidence and unresolved questions |



DRAFT FOR REVIEW

# Operating evidence over time

**01**

Authentic records support what actually occurred

**02**

Unresolved exceptions need follow-up

**03**

Historical documents need current context



DRAFT FOR REVIEW

# A sustainable program review

Changed facts and upcoming obligations
Exceptions, dependencies and accountable decisions

| Review topic | Useful outcome |
| --- | --- |
| Changed environment or service | Responsible review and affected records |
| Upcoming required activities | Named owner and correct frequency basis |
| Exceptions and missing support | Specific action and escalation |
| Ownership or personnel changes | Updated duties and knowledge handover |



DRAFT FOR REVIEW

# Practice scenario

01

A provider service changed

02

The application owner left

03

The tracker still shows last year’s evidence as complete



DRAFT FOR REVIEW

# Scenario debrief

Current facts need current responsible owners
Prior evidence remains historical unless its relevance is established

| Changed fact | Next preparation action |
| --- | --- |
| Provider service changed | Vendor owner correlates current service records |
| Application owner left | Authorized owner reassigns and communicates duties |
| Last year’s tracker status persists | Coordinator separates historical support from current work |
| Change impact is unresolved | Responsible owners document review and follow-up |



DRAFT FOR REVIEW

# Knowledge check

## Which statement is accurate?

A. Last year’s result establishes current operation

B. A monthly meeting satisfies every required frequency

C. A TRA can change any requirement’s frequency

**D. Each activity needs its own applicable timing basis**



DRAFT FOR REVIEW

# Answer and explanation

**01**

D is accurate

**02**

Internal coordination and required activity timing have distinct purposes



DRAFT FOR REVIEW

# Your program continuity brief

01

Record each activity’s owner and timing basis

02

Link current procedures and authentic records

03

Hand over open decisions and dependencies



DRAFT FOR REVIEW

# Sources and course boundary

**PCI DSS v4.0.1: sections 5 and 10**

Requirements 12.1.2–12.1.3, 12.3.1, 12.5.2–12.5.2.1

Requirements 6.5.2 and 12.8.4–12.8.5

**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