THRIVEPCI / PCI FOUNDATIONS

Accessible Text Companion

Slide text, tables, and narration script

Version 0.3.0+20261118T154700Z | 18 November 2026

> **Draft for review.** This companion presents the slide text, tables, and narration script in reading order. It is not a transcript of recorded audio. No audio or video has been produced, and timed captions remain pending a real recording. Technical review is pending.

The narration text is provided for Scott to review and record. It is not an assertion that the course has been narrated.

SLIDE 01 | COVER

PCI Foundations

- A confident first step into PCI
- Trainer edition 0.1.2+20261118T001907Z · Draft for review

NARRATION SCRIPT | NOT RECORDED AUDIO

> Welcome to ThrivePCI. This course introduces the people and preparation questions behind a PCI DSS program. We will follow a fictional business called Harbor Learning as its team prepares for a discussion about payment security. The examples contain no real customer information. You do not need a technical background to begin. Our goal is to help you ask clearer questions and recognize the work your organization owns. This course provides education. It does not determine your scope, select your reporting path or establish compliance. Keep those decisions with the appropriate responsible parties and use the current standard alongside this material.

Source note (not spoken): PCI DSS v4.0.1, sections 3, 4 and 11

Learning objectives

- Recognize the main PCI terms and roles
- Describe the organization’s preparation responsibilities
- Create a useful first discussion agenda

NARRATION SCRIPT | NOT RECORDED AUDIO

> By the end, you should be able to explain several terms without turning them into an assessment conclusion. You should also be able to separate the work of the organization from the support provided by a readiness partner or an assessor. Finally, you will prepare a short agenda for your team. Think about your current situation as we proceed, but use generic notes rather than live payment details or confidential evidence. If a term is unfamiliar, pause and write it down. The point of this introduction is to build a shared language that supports better decisions, not to memorize every requirement number.

Source note (not spoken): Practitioner teaching method

Payment security vocabulary

- PCI DSS describes security requirements and testing procedures
- The environment and services shape the questions
- Reporting instructions come from the applicable compliance program

NARRATION SCRIPT | NOT RECORDED AUDIO

PCI DSS is the Payment Card Industry Data Security Standard. Its requirements and testing procedures provide the basis for assessment work. You will also hear terms such as cardholder data environment, service provider, self-assessment questionnaire and Report on Compliance. Each term has a specific meaning in the applicable documents. Avoid choosing a reporting document simply because its name sounds familiar. PCI SSC explains that payment brands, acquirers and other organizations managing compliance programs determine reporting requirements. For Harbor Learning, the useful first task is to describe how payments work and identify who provides reporting instructions. That is a preparation task, not a scope decision made by this course.

Source note (not spoken): PCI DSS v4.0.1, sections 3, 4 and 11

Harbor Learning's payment questions

- Use facts the business can substantiate
- Record uncertainty for follow-up

Question	Possible information owner
Payment channels and business process	Operations lead
Systems and connections	Technical owner
Consumed provider service	Vendor owner
Reporting instructions	Compliance program contact

NARRATION SCRIPT | NOT RECORDED AUDIO

Harbor Learning sells online workshops. The operations lead says a payment provider handles checkout, but nobody has assembled a current description of the service. Rather than declaring the business out of scope, the team records questions. Which payment channels exist? Which provider service does the business consume? Where can staff see payment-related information? Which systems connect to the process? Who supplies compliance reporting instructions? The answers need support from the actual environment and service arrangements. On this slide, each question has a possible information owner. The table is a practical discussion aid. It does not replace the scoping confirmation required by the standard or any reporting eligibility criteria.

Source note (not spoken): PCI DSS v4.0.1, section 4 and requirement 12.5.2

People in the preparation process

- The assessed entity owns its program and submissions
- A readiness partner helps prepare
- The assessor performs the agreed assessment activities

NARRATION SCRIPT | NOT RECORDED AUDIO

> The assessed entity is the organization whose environment and practices are being evaluated. Its team owns the program and the information it presents. A readiness partner can help the organization understand preparation needs, organize evidence and work through gaps. Readiness partner is our practitioner term for that support role, not a PCI DSS mandated job title. The assessor performs the assessment activities required by the relevant engagement and reporting instructions. Keep those responsibilities clear when asking for help. An assessor's request for evidence is not automatically a commitment to create your policies, reconstruct your provider mapping or perform your remediation work.

Source note (not spoken): PCI DSS v4.0.1, sections 9–11; practitioner role model

A practical role map

- Different roles can sit with the same person
- Responsibilities still need explicit ownership

Role	Preparation contribution
Executive sponsor	Resources and escalation
Program owner	Coordination and dependencies
Control owner	Activity and supporting evidence
Vendor owner	Provider service and responsibility information

NARRATION SCRIPT | NOT RECORDED AUDIO

In a small business, one person may hold several roles. That does not remove the need to identify the work. Harbor Learning assigns an executive sponsor to resolve priority and resource questions. A program owner coordinates the preparation plan. Technical and business control owners perform their assigned activities. The vendor owner obtains service-specific information. External readiness support helps with preparation where engaged. The assessor validates the presented information through the applicable testing. This map is intentionally simple. It supplements, rather than replaces, the organization's formal security responsibilities and requirement-specific role documentation. Ask whether each responsibility has an owner who understands what is expected.

Source note (not spoken): PCI DSS v4.0.1, 12.1.3 and requirement-specific x.1.2 controls; practitioner role map

Tools and supporting evidence

- A platform can organize records and tasks
- The underlying activity still needs support
- The applicable testing procedures guide assessment

NARRATION SCRIPT | NOT RECORDED AUDIO

> A compliance automation platform can be useful. It may collect records, monitor selected conditions or organize assignments. The team must still understand what each record demonstrates. A green indicator could reflect a configured check, a submitted file or a platform-specific status. It should not be treated as a complete explanation of every PCI DSS testing objective. Harbor Learning starts by connecting the requested activity to an owner and the relevant supporting material. PCI DSS describes examination, observation and interview as assessment methods. The exact procedures determine the expected testing. Platform records can contribute, but the team should be ready to explain their relevance and limits.

Source note (not spoken): PCI DSS v4.0.1, section 10

A useful preparation record

- Describe the activity and supporting material
- Identify open questions without inventing answers

Preparation field	Illustrative entry
Activity	Review of a defined account population
Owner	Application access owner
Supporting record	Review decisions and action log
Open question	Population source still needs confirmation

NARRATION SCRIPT | NOT RECORDED AUDIO

Consider a generic access review. A preparation record can state which population the review covered, who performed it, when it occurred and where the decisions and follow-up actions are recorded. That is more useful than a file called access review with no context. This example illustrates clear presentation. It does not assert that a particular review population, frequency or document satisfies a specific requirement. The organization must align those details with the applicable requirement and testing. Harbor Learning keeps an unresolved question beside the record if it cannot yet explain the population or period. Uncertainty should lead to an owned follow-up, not a guessed assertion.

Source note (not spoken): PCI DSS v4.0.1, section 10; practitioner evidence presentation

Practice scenario

- A provider handles checkout
- The dashboard shows green
- No current process description exists

NARRATION SCRIPT | NOT RECORDED AUDIO

> Pause here and consider Harbor Learning’s first team meeting. The founder says the provider handles checkout and the dashboard is green, so preparation should be complete. The program owner has no current payment-process description, no provider responsibility mapping and no confirmed reporting instructions. What should the team do next? Take two minutes to write three questions and assign a generic owner to each. Do not decide that the business is compliant, non-compliant or outside scope from these facts. The information is deliberately incomplete. Your task is to identify the next useful preparation work, using people who can substantiate the answers.

Source note (not spoken): Practitioner exercise based on PCI DSS v4.0.1, sections 4, 10 and 11

Scenario debrief

- A clearer question creates a useful next step
- Evidence and reporting decisions need the right parties

Next question	Owner and expected output
How do payments move?	Operations: process description
Which service do we consume?	Vendor owner: service-specific documents
Who sets reporting instructions?	Program owner: confirmed program contact
What remains unresolved?	Program owner: owned question register

NARRATION SCRIPT | NOT RECORDED AUDIO

A useful response begins with facts about the payment process. Operations can describe the channels and customer journey. The vendor owner can identify the consumed service and obtain appropriate provider documentation. The program owner can confirm which organization supplies reporting instructions and collect the unresolved questions. Technical staff can help explain systems and connections. None of these actions automatically settles scope or reporting eligibility. The team is improving the inputs for the appropriate review. Notice that every question has an owner and an expected output. This reduces the risk of a meeting ending with a general request for someone to look into PCI.

Source note (not spoken): PCI DSS v4.0.1, section 4, section 11 and 12.8; practitioner debrief

SLIDE 11 | QUESTION

Knowledge check

- Which statement is best supported?
- A. Green dashboard means compliance
- B. Provider checkout removes every responsibility
- C. The team needs substantiated facts and reporting instructions
- D. The assessor must build the program

NARRATION SCRIPT | NOT RECORDED AUDIO

> Choose the statement that is best supported by what we know. A says the dashboard establishes compliance. B says using a provider removes every responsibility. C says the team needs substantiated facts about its environment and the relevant reporting instructions. D says the assessor must build the program. Pause before advancing and explain your choice in one sentence. This is a learning check, not a compliance score. The useful reasoning is more important than selecting a letter. Ask which statement respects the limits of the information available and assigns the organization a practical next step without inventing an outcome.

Source note (not spoken): Practitioner learning check

Answer and explanation

- C is the supported answer
- The other choices make claims the scenario cannot support

NARRATION SCRIPT | NOT RECORDED AUDIO

> C is the supported answer. Harbor Learning needs reliable facts about the process and the reporting instructions that apply to its compliance program. A platform status can help direct attention, but the scenario does not show that all applicable requirements and testing have been satisfied. A provider can perform activities for the business, yet the business still needs to understand its retained and shared responsibilities. An assessment engagement also does not automatically include building the program. If you selected a different answer, identify the assumption you added. That habit is valuable in preparation work because unsupported assumptions often hide behind familiar tools, supplier names or last year's documents.

Source note (not spoken): PCI DSS v4.0.1, sections 4, 10 and 11; requirements 12.8.4–12.8.5

Your first preparation agenda

- Describe the process and information owners
- List provider and reporting questions
- Assign the next action and review point

NARRATION SCRIPT | NOT RECORDED AUDIO

> Your practical takeaway is a one-page meeting agenda. Start with the business payment process in plain language. Name the people who can explain the systems, services and reporting instructions. List what you know, what evidence supports it and what still needs confirmation. Give each open question an owner and a review point. Use generic or redacted examples in training and keep real customer records in approved channels. This agenda is a practitioner preparation tool. It does not replace formal scope documentation, security responsibilities or an assessment report. A good first meeting ends with work that someone can perform and an output the team can review.

Source note (not spoken): Practitioner preparation method

Sources and course boundary

- PCI DSS v4.0.1: sections 3, 4, 9, 10 and 11
- Requirements 12.1.3, 12.5.2 and 12.8
- Practitioner examples and role model

NARRATION SCRIPT | NOT RECORDED AUDIO

> The reference baseline for this course is PCI DSS version 4.0.1, Requirements and Testing Procedures, published by PCI SSC in June 2024. The cited introductory sections explain terminology, scope, assessment practices and reporting context. The cited requirements support our discussion of responsibilities, scoping confirmation and third-party services. Our role map, agenda and fictional examples are practitioner teaching aids. They are not additional Council requirements or an endorsement by PCI SSC or another organization. Use the current authoritative documents and the instructions of the appropriate responsible parties when applying the ideas. The deck remains a review draft and does not guarantee compliance or a favorable assessment.

Source note (not spoken): PCI DSS v4.0.1, supplied project source; practitioner guidance

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