

Course Syllabus/Outline

Payment Card Industry Data Security Standard (PCI DSS): Primer Course

Course Description and Goals

Course Description: This course focuses on the fundamentals of the Payment Card Industry (PCI) and how the security of the data captured (specifically customer credit card data) protects merchants and service providers each and every day. The PCI DSS (Data Security Standard), now in version 4.0, provides a comprehensive review of the changes and updates provided by the Data Security Council in this latest release. Whether you are an individual new to the PCI experience or an organization working to maintain compliance in meeting these requirements, this course is for you.

The drive behind the design and development of this course centers around allowing learners the opportunity to familiarize themselves with the process of PCI, the history behind it, the need for updating it, and the practical uses of applying these standards in everyday contexts. Designed as an introduction to a more comprehensive active practitioner based course, this introduction provides a foundational, high-level overview of the important areas that you need to focus on as the version 4.0 rules become the new standard across this industry.

Course Goals: By the end of this course, learners should be able to:

- Identify the key updates provided in the new version (version 4) of the PCI Data Security Standard (PCI DSS).
- Analyze the importance of earning and maintaining PCI compliance as part of an organizational security improvement standard.
- Identify the requirements of merchants and service providers in protecting customer cardholder data in the latest version of the PCI DSS.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Evaluate the points identified in the “path of a payment transaction” and determine the security vulnerabilities within each.
- Contrast the differences (if any) between organizations that either self-certify through a Self Assessment Questionnaire or work with a QSA to complete an annual PCI security assessment.

Areas of Course Study:

- The History of PCI
- The 6 Goals of PCI
- The 12 Main Requirements of PCI
- The Requirements of Compliance for Merchants & Service Providers
- Payments & Card Transactions
- Protecting Cardholder Data
- Working with a Qualified Security Assessor (QSA)
- Completing a PCI Assessment

For more information on the information covered in this course, please review the Detailed Course Module Outline

What You Will Receive (Key Takeaways/Real-World Skills):

- Improved perception of how PCI compliance creates a holistic view of security and reducing risk.
- Best-case guidelines for applying PCI standards (across a set of over 400 controls) and working with your QSA during an annual assessment.
- Improved understanding of how maintaining PCI compliance (as a merchant or service provider) builds trust with customers and reduces fraudulent activity.
- Best-case guidelines for using PCI compliance to meet a variety of other security standards based on the specific requirements of your organization.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Course Schedule (by Module)

Module 1	Module 2	Module 3
The Beginner's Guide to PCI DSS 4.0	What is PCI? Overview of the PCI Requirements	The Key Players Involved in the PCI Process
Meet Your Senior Instructor, Jeff Man (Video)	The View of PCI from a Qualified Security Assessor (QSA) (Video)	PCI and Merchants (Video)
Why Should You Take This Course? (Video)	PCI Data Security Standard (Video)	PCI and Service Providers (Third Party Agents) (Video)
What's New in PCI DSS 4.0? (Resources & Infographics)	How Do You Approach PCI? (Video)	
Video Series: Talking PCI 4.0 (Video)	PCI as a Daily Standard, Not Just a Yearly Assessment (Video)	
Video Series: PCI 4.0 as a Security Framework (Video)	Working With Your QSA: Identifying Your "Connected Systems" (Video)	
	Applying the PCI Security Standard (Video)	
	Explaining the Role of Encryption in PCI DSS (Video)	

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Detailed Course Module Outline

Module 1 | The Beginner's Guide to PCI DSS 4.0

Keywords: PCI DSS 3.0, PCI DSS 4.0, Reducing Risk, Security Frameworks

Module Sections:

- Meet Your Senior Instructor, Jeff Man
- Why Should You Take This Course?
- What's new in PCI DSS 4.0?
- Video Series: Talking PCI 4.0
- Video Series: PCI 4.0 as a Security Framework

Activities:

- Instructor Videos
- Infographics, Links, and Related Resources

Module Objectives:

- Identify the key changes between version 3 and version 4 of the PCI Data Security Standard (PCI DSS).
- Analyze the themes of the PCI DSS to determine how it can fit into your organizational security framework.
- Review the supporting resources (infographics, webinars) highlighting the version 4 PCI updates.
- Create a short list of key questions dealing with how to apply the PCI DSS standard.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Module 2 | What is PCI? Overview of the PCI Requirements

Keywords: Qualified Security Assessors (QSA), Applying PCI, Security Frameworks, Encryption Standards

Module Sections:

- The View of PCI from a Qualified Security Assessor (QSA)
- PCI Data Security Standard
- How Do You Approach PCI?
- PCI as a Daily Standard, Not Just a Yearly Assessment
- Working With Your QSA: Identifying Your “Connected Systems”
- Applying the PCI Security Standard
- Explaining the Role of Encryption in PCI DSS

Activities:

- Instructor Videos
- Infographics, Links, and Related Resources

Module Objectives:

- Connect with your Senior Instructor (Jeff Man) as he discusses his career as a Qualified Security Assessor (QSA).
 - Identify key terms (like scope, risk reduction) related to the application of the PCI DSS.
 - Define the role of encryption in PCI and how encryption factors into point of sale and endpoint protected devices.
 - Apply standards of PCI as part of a risk reduction strategy and not just a yearly assessment.
-

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Module 3 | The Key Players Involved in the PCI Process

Keywords: Merchants, Service Providers, Self Assessment Questionnaires, Merchant Classification Levels

Module Sections:

- PCI and Merchants
- PCI and Service Providers (Third Party Agents)

Activities:

- Instructor Videos
- Infographics, Links, and Related Resources

Module Objectives:

- Identify the levels of merchants according to current PCI standards.
 - Review situations when merchants can either submit to a PCI Assessment or completing a Self Assessment Questionnaire.
 - Analyze the impact (from a Merchant/Service Provider perspective) of transmitting, processing, or storing customer information and payment card data.
 - Analyze potential classification changes for both merchants and service providers coming in the version 4 update.
-

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.