Payment Card Industry (PCI) Risk Essentials Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern digital economy thrives on secure payment processing, yet organizations face an ever-increasing barrage of cyber threats and complex regulatory mandates. The Payment Card Industry Data Security Standard (PCI DSS) is the cornerstone of protecting Cardholder Data from compromise. Payment Card Industry (PCI) Risk Essentials Training Course is designed to instill a security-first culture across all personnel involved in the Cardholder Data Environment (CDE). By focusing on PCI DSS v4.0 principles, risk management fundamentals, and compliance maintenance, we empower employees to become the first line of defense against costly data breaches, ensuring organizational adherence to the standards set by the PCI Security Standards Council (PCI SSC) and protecting customer trust.

This intensive course moves beyond simple awareness to deliver practical, actionable knowledge in payment security and risk mitigation. Participants will master the critical concepts of scope definition, secure handling of Sensitive Authentication Data (SAD), and the importance of continuous compliance. Utilizing real-world case studies and interactive modules, the training clarifies the specific security obligations under the evolving standard, including requirements for Zero Trust principles, Multi-Factor Authentication (MFA), and third-party vendor risk management. Successful completion will equip participants with the skills to effectively identify, assess, and manage risks, thereby fortifying their organization's overall security posture and simplifying future Qualified Security Assessor (QSA) audits.

Programme Curriculum

Payment Card Industry (PCI) Risk Essentials Training Course

Introduction

The modern digital economy thrives on secure payment processing, yet organizations face an ever-increasing barrage of cyber threats and complex regulatory mandates. The Payment Card Industry Data Security Standard

(PCI DSS) is the cornerstone of protecting Cardholder Data from compromise. Payment Card Industry (PCI) Risk Essentials Training Course is designed to instill a security-first culture across all personnel involved in the Cardholder Data Environment (CDE). By focusing on PCI DSS v4.0 principles, risk management fundamentals, and compliance maintenance, we empower employees to become the first line of defense against costly data breaches, ensuring organizational adherence to the standards set by the PCI Security Standards Council (PCI SSC) and protecting customer trust.

This intensive course moves beyond simple awareness to deliver practical, actionable knowledge in payment security and risk mitigation. Participants will master the critical concepts of scope definition, secure handling of Sensitive Authentication Data (SAD), and the importance of continuous compliance. Utilizing real-world case studies and interactive modules, the training clarifies the specific security obligations under the evolving standard, including requirements for Zero Trust principles, Multi-Factor Authentication (MFA), and third-party vendor risk management. Successful completion will equip participants with the skills to effectively identify, assess, and manage risks, thereby fortifying their organization's overall security posture and simplifying future Qualified Security Assessor (QSA) audits.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Interpret PCI DSS v4.0 requirements and their impact on daily operations.
2. Accurately define and scope the Cardholder Data Environment (CDE).
3. Implement strong access control measures, focusing on least privilege.
4. Understand the necessity and application of Multi-Factor Authentication (MFA) for all system access.
5. Apply proper handling, storage, and data retention policies for Cardholder Data.
6. Identify and mitigate common supply chain and third-party vendor risks associated with payment processing.
7. Analyze real-world data breach case studies to prevent similar future incidents.
8. Recognize and report potential phishing and social engineering threats.
9. Comprehend the role of Tokenization and Point-to-Point Encryption (P2PE) in reducing PCI scope.
10. Support and participate in the annual risk assessment and compliance validation processes
11. Apply secure configuration and vulnerability management practices to payment systems.
12. Contribute to an organizational security-first culture and continuous monitoring efforts.
13. Understand the differences between CHD and Sensitive Authentication Data (SAD) and the prohibition on SAD storage.

Target Audience

1. IT/System Administrators and Network Operations Staff
2. Compliance Officers and Internal Auditors
3. Customer Service Representatives and Call Center Agents
4. Security Analysts and Risk Management Professionals
5. Software Developers and Quality Assurance Testers
6. Department Managers
7. Executives and Project Managers overseeing payment systems.
8. All employees with access to the Cardholder Data Environment (CDE).

Course Modules

Module 1: Introduction to PCI DSS and Scope

- Overview of the PCI Security Standards Council and its role.
- Understanding the ecosystem.
- Cardholder Data (CHD) and Sensitive Authentication Data.
- Defining and reducing the Cardholder Data Environment scope.
- Case Study: Analyzing a breach caused by a failure in CDE scope definition

Module 2: The Evolving Standard: PCI DSS v4.0

- Key changes from v3.2.1 to the current PCI DSS v4.0 standard.
- Focus on customized approach and increased flexibility.
- New requirements for Targeted Risk Analyses and controls.
- Emphasizing continuous compliance over annual compliance snapshots.
- Case Study: The impact of not adopting new MFA and password requirements in a timely manner.

Module 3: Cardholder Data Protection

- The 12 PCI DSS Requirements.
- Protecting Stored Cardholder Data
- Protecting Cardholder Data in Transit
- Prohibited storage of Sensitive Authentication Data
- Case Study: A hotel chain breach illustrating failure to adequately encrypt data at rest.

Module 4: Access Control and Authentication

- Implementing Multi-Factor Authentication for all non-console access.
- Creating and managing unique user IDs and strong passwords/passphrases.
- Applying the principle of least privilege to all system components.
- Controlling physical access to the CDE and all media.
- Case Study: An internal employee breach due to shared accounts and lack of MFA on critical systems.

Module 5: Network Security and Vulnerability Management

- Building and maintaining secure networks with firewalls and secure configuration.
- Protecting systems from malware and ensuring prompt patch management.
- Regular vulnerability scanning and penetration testing.
- Securing wireless access and vendor-supplied defaults.
- Case Study: The Equifax breach demonstrating a failure in prompt patch management for a known vulnerability.

Module 6: Third-Party and Vendor Risk

- The importance of due diligence for Third-Party Service Providers
- Understanding the shared responsibilities matrix with service providers.
- Monitoring and maintaining a list of all vendors in the CDE.
- Ensuring vendors meet PCI DSS obligations.
- Case Study: Analyzing a breach originating from a compromised Third-Party Payment Processor.

Module 7: Security Awareness and Incident Response

- Implementing effective security awareness training for all personnel.
- Identifying and reporting security incidents, including phishing and social engineering.
- Developing and testing an Incident Response Plan
- Log management and monitoring for suspicious activity.
- Case Study: The RSA SecurID breach, emphasizing the role of targeted social engineering and the response required.

Module 8: Compliance Validation and Maintenance

- Self-Assessment Questionnaires and Report on Compliance
- Selecting the correct SAQ type to accurately reflect CDE scope.
- Maintaining documentation and evidence for auditors
- The role of the Qualified Security Assessor
- Case Study: A company facing fines due to using an incorrect SAQ and lacking required documentation.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com