PCI DSS v4.0 Implementation and Auditing Training Course.

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The Payment Card Industry Data Security Standard v4.0 marks a significant evolution in global payment cybersecurity and risk management. PCI DSS v4.0 Implementation and Auditing Training Course. is designed to equip security, IT, and compliance professionals with the in-depth technical expertise and strategic knowledge required to successfully implement, manage, and audit the new security controls. With a critical transition period ending, proactive compliance readiness is paramount to protecting the Cardholder Data Environment and avoiding severe financial and reputational consequences. The course shifts the focus from a purely compliance-based checklist to a continuous security process, emphasizing new requirements like the Customized Approach, Targeted Risk Analysis (TRA), enhanced authentication controls (MFA), and secure development practices.

This program provides a practical, auditor-centric perspective on the Standard, ensuring participants not only understand the 12 core requirements but can also effectively scope, reduce risk, and validate adherence using the latest PCI SSC methodologies. Leveraging real-world breach scenarios and implementation challenges, we foster a robust understanding of how to build and maintain a sustainable security program. Successful completion certifies expertise in the latest threat landscape mitigation, enabling professionals to champion organizational resilience and confidently demonstrate compliance to Qualified Security Assessors (QSAs) and internal stakeholders, securing the future of their organization's payment ecosystem.

Programme Curriculum

PCI DSS v4.0 Implementation and Auditing Training Course.

Introduction

The Payment Card Industry Data Security Standard v4.0 marks a significant evolution in global payment cybersecurity and risk management. PCI DSS v4.0 Implementation and Auditing Training Course is designed to equip security, IT, and compliance professionals with the in-depth technical expertise and strategic knowledge required to successfully implement, manage, and audit the new security controls. With a critical transition period ending, proactive compliance readiness is paramount to protecting the Cardholder Data Environment and avoiding severe financial and reputational consequences. The course shifts the focus from a purely compliance-based checklist to a continuous security process, emphasizing new requirements like the Customized Approach, Targeted Risk Analysis (TRA), enhanced authentication controls (MFA), and secure development practices.

This program provides a practical, auditor-centric perspective on the Standard, ensuring participants not only understand the 12 core requirements but can also effectively scope, reduce risk, and validate adherence using the latest PCI SSC methodologies. Leveraging real-world breach scenarios and implementation challenges, we foster a robust understanding of how to build and maintain a sustainable security program. Successful completion certifies expertise in the latest threat landscape mitigation, enabling professionals to champion organizational resilience and confidently demonstrate compliance to Qualified Security Assessors (QSAs) and internal stakeholders, securing the future of their organization's payment ecosystem.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Master the PCI DSS v4.0 Framework and its core principles for Payment Security.
2. Accurately Scope the Cardholder Data Environment (CDE) and apply segmentation techniques for scope reduction.
3. Implement new and evolving controls, especially those focused on Phishing and E-commerce Security.
4. Conduct a Targeted Risk Analysis (TRA) for periodic and customized requirements.
5. Apply the Customized Approach effectively and understand the new Control Objectives.
6. Design and maintain robust Network Security Controls and secure configurations
7. Deploy modern solutions for Account Data Protection, including Tokenization and Encryption
8. Implement advanced Vulnerability Management and Secure Software Development Life Cycle (SSDLC) practices
9. Configure and audit Strong Authentication Controls, including mandatory Multi-Factor Authentication
10. Ensure Physical Security Controls are integrated with digital security policies
11. Establish comprehensive Logging and Monitoring strategies to detect security events
12. Design and execute effective Security Testing methodologies, including penetration testing
13. Develop and manage the required Information Security Policies and Compliance Readiness programs

Target Audience

1. Information Security Managers and Officers
2. PCI DSS Project Managers/Lead Implementers
3. Internal Security Assessors (ISAs)
4. IT Directors and Operations Staff
5. Compliance, Risk, and Audit Professionals
6. Security Engineers and Architects
7. System Administrators and Network Engineers

8. Third-Party Service Provider (TPSP) Personnel

Course Modules

1. Introduction to PCI DSS v4.0 and Scoping

- Key changes from v3.2.1 to v4.0 and the Transition Timeline.
- Understanding the new Security as a Continuous Process model.
- Defining the Cardholder Data Environment and Connected-To systems.
- Segmentation strategies for Scope Reduction and their audit validation.
- Overview of the new reporting options
- Case Study: Analysis of a large e-commerce retailer?ÇÖs successful CDE de-scoping project post-v4.0 to minimize compliance burden and costs.

2. Risk Management and Customized Approach

- Mastering the Targeted Risk Analysis methodology for periodic reviews.
- The principles of the Customized Approach and its documentation requirements.
- Developing and evaluating Compensating Controls under v4.0.
- Integrating PCI DSS into a broader Enterprise Risk Management framework.
- Preparing the necessary Risk Analysis Template and evidence for a QSA.
- Case Study: Examining a multi-national service provider's use of the Customized Approach to achieve a security objective where a required control wasn't technically feasible.

3. Network and Security Controls

- Implementing and auditing Network Security Controls
- Protecting the CDE with robust Secure Network Architectures.
- Applying Secure Configurations to all system components, including hardening standards.
- New requirements for network monitoring and Outbound Traffic Filtering.
- Inventory management for all in-scope system components.
- Case Study: Review of a financial processor that failed an audit due to undocumented changes in a secure configuration baseline and the remediation steps taken.

4. Data Protection and Storage

- Identifying and protecting all forms of Stored Account Data, including PAN, Track Data, and the PCI DSS 4.0 storage requirements.
- Implementing Cryptography and key management for data-at-rest protection.
- Best practices for Tokenization and Truncation for PAN protection.
- Securing data in-transit with strong encryption.
- Data retention and secure disposal policies.
- Case Study: Analyzing a major data breach caused by unencrypted Primary Account Numbers in system logs and the v4.0-mandated log management and encryption solution implemented.

5. Malware and Secure Software

- Enhanced requirements for anti-malware and anti-virus solutions on system components.
- New requirements for performing Automated Malware Scanning and active checking.
- Integrating security into the Secure Software Development Life Cycle.
- Addressing high-risk vulnerabilities promptly and using a vulnerability ranking system.
- Implementing a formal Change Control Process that includes security validation.

- Case Study: The audit findings for a custom application with a severe Injection Vulnerability and the v4.0 requirement for Secure Coding Training and security testing integration.

6. Access Control and Authentication

- Applying the Least Privilege and Need-to-Know principles to access.
- Mandatory Multi-Factor Authentication for all CDE access and non-console administrative access.
- Managing user IDs and Password/Passphrase requirements
- Controls for application and system accounts, including service accounts.
- Reviewing user access and maintaining privileged access policies.
- Case Study: A case demonstrating the implementation of MFA for all in-scope personnel and service providers to meet the v4.0 mandates and how this was validated in an audit.

7. Physical and Logging Security

- Restricting Physical Access to the CDE and sensitive facilities.
- Visitor access control and physical media controls
- Requirement for Automated Audit Logs for all system components and critical events.
- Log Monitoring and review procedures, including new requirements for security event monitoring.
- Time synchronization and secure storage of audit logs
- Case Study: An internal audit finding where unmonitored server room access led to a security gap, highlighting the necessity of integrated digital and physical controls.

8. Testing and Validation

- Implementing a formal, risk-based program for Vulnerability Scanning
- Penetration Testing methodologies and scoping requirements.
- New requirements for E-commerce Skimming and detecting malicious scripts
- Utilizing Intrusion Detection/Prevention Systems and file integrity monitoring.
- Wireless access management and wireless vulnerability testing.
- Case Study: Demonstrating the impact of a new E-commerce Skimming detection requirement on a payment gateway and how they used a Targeted Risk Analysis to define its review frequency.

9. Policy and Program Management

- Developing and maintaining the Information Security Policy framework.
- Managing Third-Party Service Provider relationships and compliance.
- Mandatory Security Awareness Training and review requirements.
- Formalized Incident Response Plan development, testing, and review.
- Annual confirmation of PCI DSS Scope
- Case Study: A review of a TPSP that failed to provide sufficient documentation of its security controls and the merchant's required due diligence and reporting process under v4.0.

10. Requirement 1: Network Security Controls

- Detailed breakdown of firewall and router configuration standards.
- Securely segregating the CDE from out-of-scope networks.
- New controls for preventing disclosure of cardholder data via outbound traffic.
- Reviewing firewall rules every six months.
- Technical implementation and auditing checklist.

- Case Study: A scenario involving a misconfigured firewall rule that inadvertently exposed a database server and the v4.0 mandate for stricter, formalized configuration management.

11. Requirement 2: Secure System Components

- Changing all vendor-supplied defaults on new and existing systems.
- Developing and maintaining configuration standards.
- Managing inventory of all in-scope system components.
- New requirements for shared hosting providers.
- Audit procedures for secure configurations.
- Case Study: The process and documentation required for a successful audit demonstrating that all new systems had been hardened using an approved security benchmark.

12. Requirement 3: Protect Stored Account Data

- Implementing effective data retention and disposal policies.
- Masking the PAN when displayed and the new masking requirements.
- Strong cryptography implementation guidance.
- Cryptographic key management procedures.
- Auditing data storage locations and encryption strength.
- Case Study: Analyzing a breach where PAN data was improperly stored in a flat file outside of the CDE, focusing on v4.0?ÇÖs zero-tolerance for Sensitive Authentication Data storage.

13. Requirement 5: Protect from Malicious Software

- Configuring anti-malware to perform active scanning and updates.
- New Requirement 5.3.2.1 for anti-malware on endpoints not traditionally considered targets.
- Monitoring anti-malware and audit log reviews.
- Processes for addressing identified malicious software.
- Implementing a formalized process for managing anti-malware solution failures.
- Case Study: A scenario detailing an attack where an endpoint outside the CDE was compromised, leading to CDE access, and how the new requirement would have mitigated this risk.

14. Requirement 6: Secure Systems and Software

- Prioritizing and addressing critical security patches within 30 days.
- Formal change control and testing processes for all system changes.
- Implementing secure coding practices and training for developers.
- Using automated tools for vulnerability detection.
- Auditing the secure software development lifecycle.
- Case Study: A development team's transition to a new CI/CD pipeline and how they integrated security testing and static code analysis to comply with v4.0's strengthened Req 6.

15. Audit and Reporting Essentials

- The role of the Qualified Security Assessor and the Internal Security Assessor
- Preparing the Report on Compliance and supporting documentation.
- The validation process for merchants and service providers.
- Common audit failures and how to avoid them under v4.0.
- Maintaining Continuous Compliance and the quarterly review process.

- Case Study: A mock audit simulation, reviewing a company's documentation and identifying gaps in evidence for the Customized Approach and Targeted Risk Analysis.

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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