multisoft
Systems

PCI-DSS Practitioner Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

☎ (+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The PCI-DSS Practitioner Training by Multisoft Systems is designed to equip professionals with the knowledge and hands-on skills required to implement, manage, and maintain compliance with the Payment Card Industry Data Security Standard (PCI-DSS). As digital transactions grow globally, ensuring the security of cardholder data has become a top priority for businesses, financial institutions, and service providers.

Module 1: Introduction to PCI-DSS

- ✓ Understanding Payment Card Industry ecosystem
- ✓ Why PCI-DSS exists: purpose, scope & objectives
- ✓ Overview of card brands & PCI Security Standards Council
- ✓ Key PCI standards: DSS, P2PE, PIN, 3DS, PA-DSS
- ✓ Compliance responsibilities for merchants, processors & service providers

Module 2: PCI-DSS Framework & Requirements

- ✓ Structure of PCI-DSS: 12 Requirements
- ✓ Overview of 6 control objectives
- ✓ Mandatory controls & security expectations
- ✓ Applicability to various business types
- ✓ Mapping PCI controls to business environments

Module 3: PCI-DSS Scoping and Segmentation

- ✓ Determining cardholder data environment (CDE)
- ✓ Identifying in-scope and out-of-scope components
- ✓ Network segmentation best practices
- ✓ Reducing compliance burden through proper scoping
- ✓ Real-world scoping examples

Module 4: Understanding Cardholder Data (CHD) & Sensitive Authentication Data (SAD)

- ✓ Difference between CHD and SAD
- ✓ Allowed vs prohibited data storage
- ✓ Tokenization & encryption mechanisms
- ✓ Data masking standards
- ✓ CHD lifecycle and security considerations

Module 5: PCI-DSS Requirement Deep Dive (1–6)

- ✓ Tools, techniques & best practices for each requirement

Module 6: PCI-DSS Requirement Deep Dive (7–12)

- ✓ Practical controls, monitoring tools & documentation needed

Module 7: Authentication, Encryption & Key Management

- ✓ Cryptographic key management policies
- ✓ TLS best practices
- ✓ Secure credential management
- ✓ Multi-factor authentication (MFA) requirements
- ✓ Common encryption algorithm standards

Module 8: Risk Assessment & Vulnerability Management

- ✓ Conducting PCI-aligned risk assessments
- ✓ Vulnerability scanning (ASV)
- ✓ Internal vs external pen testing requirements
- ✓ Remediation and documentation
- ✓ Secure patching practices

Module 9: PCI-DSS Compliance Levels & Validation

- ✓ Merchant levels (1–4)
- ✓ Service provider categories
- ✓ When PCI audit is mandatory
- ✓ Understanding ROC, SAQ, AOC, ASV reports
- ✓ Choosing the appropriate SAQ type

Module 10: Incident Response & Breach Handling

- ✓ Creating PCI-compliant incident response plan
- ✓ Identifying and containing card data breaches
- ✓ Forensic investigation requirements
- ✓ Role of PFI (PCI Forensic Investigator)
- ✓ Mandatory reporting timelines

Module 11: Documentation & Evidence Collection

- ✓ Mandatory policies & procedures
- ✓ Evidence required for each PCI control
- ✓ Audit-ready documentation
- ✓ Common gaps & how to avoid them

Module 12: Tools & Technologies for PCI Compliance

- ✓ DLP, SIEM, IDS/IPS, NAC
- ✓ Encryption/tokenization tools
- ✓ Logging and monitoring solutions
- ✓ Vulnerability scanners
- ✓ Secure coding platforms