Role-based PCI DSS Compliance Training

The Payment Card Industry Data Security Standard (PCI DSS) is a set of internationally applicable standards designed to ensure any entity that stores, processes, or transmits cardholder data maintains a secure environment. This course introduces the concept of PCI DSS then provides role-specific guidance for those who have a direct function in ensuring your organization is PCI DSS compliant.

PCI DSS has traditionally been a difficult standard to cover in an enterprise-wide manner since each learner's responsibilities, as they relate to the mandate, will vary significantly from role to role across the organization. The struggle for security awareness teams has been in getting the most out of a limited instruction window while making sure training is relevant to each learner.

How it Works

Ensure your employees receive the training they need by assigning modules based on their specific roles. It's recommended all employees complete the PCI DSS Introduction, followed by the module relevant to their job responsibilities. Our training simplifies compliance by providing clear and relevant information for every level of your organization.

Navigating the New Standards: Key Changes in PCI DSS 4.0

More Documentation and Reporting

- Organizations must maintain more comprehensive documentation and reporting of security controls and processes.
- Required to show how you meet PCI DSS requirements and provide evidence of ongoing compliance efforts.

More Comprehensive Risk-Based Security Approach

- Additional requirements to better identify and protect sensitive data.
- Ensure the integrity of systems and applications.
- Maintain ongoing monitoring and implement incident response plans.

More Flexibility in Meeting Requirements

- Organizations can choose a more customized approach using innovative methods to achieve their security goals.

Ongoing Risk Assessment

- Continuous evaluation and identification of emerging risks and vulnerabilities.
- Adjust security controls accordingly to reflect the changing threat landscape.

Expanded Scope of Testing

- In addition to annual penetration testing, regular vulnerability scans are required.
- Implement a process for identifying and addressing vulnerabilities in systems and applications.

Enhanced Authentication

- Multi-factor authentication (MFA) is now required for all personnel with local or remote access to all systems and applications in the cardholder data environment.

Third-Party Service Provider Management Process

- Formal process required for ongoing monitoring, management, and ensured security of third-party service providers interacting with the cardholder data environment.

Tailored PCI DSS Training for Every Role

In this course, a selection of up to seven animated modules can be assigned based on the unique roles and responsibilities of the members of your organization. As you choose the training that's right for each person, you can be confident that employees will not be over trained, and the curriculum will relate appropriately to each learner's responsibilities. Each module in the course is authored by SANS subject-matter experts and leverage the engaging and effective learning format users expect from SANS Workforce Security & Risk Training.

Module Name	Description	Typical Roles
PCI DSS Introduction	Introduces PCI DSS, a set of standards for protecting cardholder data. Covers the definition of cardholder data, technical and operational requirements, and best practices for compliance. Emphasizes the importance of data protection and compliance.	All employees.
PCI DSS for Application Development Teams	Equips development teams with PCI DSS compliance skills. Focuses on network security, system configurations, encryption, secure software practices, access controls, and regular monitoring. Emphasizes documentation for audits.	E-commerce web developers, application development team members, and database or enterprise developers.
PCI DSS for Customer-Facing Employees	Empowers frontline staff to protect cardholder data during transactions. Covers secure payment device use, data access management, and proper data disposal. Stresses the importance of reporting unusual activities.	Customer sales and support staff, cashiers, payment processors, and customer service representatives.
PCI DSS for Managers	Provides managers with tools to enforce PCI DSS compliance. Focuses on limiting data access, encouraging security communication, and maintaining data protection. Covers secure access approvals and compliance collaboration.	Team leads, executives, department managers, directors, store managers, vendor managers, and customer experience specialists.
PCI DSS for Back-Office Employees	Empowers back-office staff to protect cardholder information. Covers secure data access, device use, data retention, and security protocols. Emphasizes error reporting and maintaining a secure environment.	Accounting and finance staff, customer service representatives, and research analysts.
PCI DSS for IT System Administrators	Details PCI DSS compliance for system administrators. Focuses on secure networks, data encryption, access controls, and vulnerability management. Covers security control implementation and compliance monitoring.	Systems administrators, service and repair specialists, computer systems analysts, and IT administrators.
PCI DSS for IT Network Administrators	Guides network administrators on PCI DSS compliance. Focuses on network security, system configurations, and encryption protocols. Emphasizes firewall installation, managing network diagrams, and documenting changes for audits.	Network administrators, network engineers, and IT support staff.