PCI101 - PCI-DSS 4.0 COMPLIANCE

Course Learning Objectives

This course is divided into four modules. The first covers an introduction to PCI DSS, where we'll identify which systems are covered by PCI DSS rules, explain how PCI DSS is structured, and describe the importance of a strong security policy. In module two, we'll look at sensitive credit card information where you'll learn how to classify data and identify its regulatory requirements, mask credit card numbers, encrypt cardholder data before storing or transmitting it, and implement physical security measures. The third module will focus on controlling access to the cardholder data environment by limiting what administrators and users can do by following the principle of least privilege, setting secure password policies, and following strong authentication practices for users and applications. Finally, the last module will cover securing your network and system components through network security controls, hardening the OS, maintaining systems, and analyzing log records.

Description

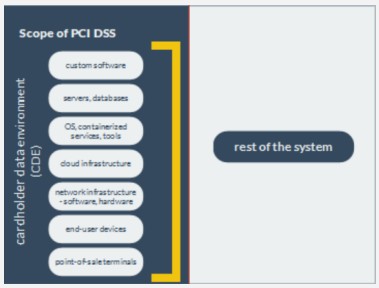
This course was designed for developers whose organizations and applications must comply with PCI DSS.

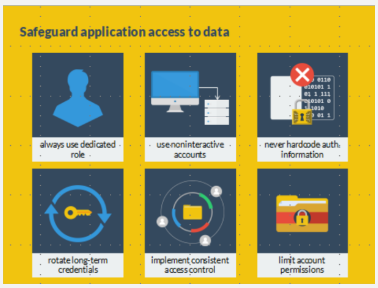
Audience

Developers
General Staff

Time Required

Tailored learning - 70 minutes approx.





PCI101 - PCI-DSS 4.0 COMPLIANCE

Course Outline

1. Planning for PCI DSS

- Overview
- What does PCI DSS cover?
- The 12 PCI DSS requirements
- Why are the requirements so broad?
- PCI DSS compliance
- Optional quiz
- Scope of PCI DSS
- Segmentation
- Implement an organizational security policy
- Secure development processes
- Maintain your security policy
- The business-as-usual (BAU) philosophy
- Keeping PCI DSS documentation secure
- Reduce your risk
- Summary

2. Safely Handling Cardholder Data

- What is cardholder data?
- Types of credit card data
- Data labeling
- Best practices for data
- What not to do
- What is masking?
- Partial masking
- Protect stored PANs
- Encryption methods
- Protect data during transmission
- In-transit vs At-rest
- Restrict physical access to data
- Physical security controls
- Summary

3. Protecting the Cardholder Data Environment

- Understanding the CDE
- Who has access to CDE?
- Principle of least privilege
- Best practices for access control
- Scenario
- Password rules
- Authentication best practices
- Application access to data
- Safeguard application access to data
- Summary

4. Network and System Requirements

- Overview – Protecting systems
- Scenario
- Network Security Controls (NSCs)
- NSCs in a cloud-based deployment
- Know your network
- Wireless access
- Hardening the OS
- Malicious software
- Maintain and update system components
- Software patches
- Incident response
- Good logging strategy
- PCI DSS rules for logging
- Summary

SecurityCompass