PCI102 - PCI SECURE SOFTWARE LIFECYCLE

Course Learning Objectives

By the end of this course, you will be able to:

- define and assign security responsibilities and resources
- develop security policies that continually monitor and improve software security
- protect critical software assets and defend against vulnerabilities
- maintain the confidentiality and integrity of payment software
- communicate guidance, security issues, and change summaries

Description

The Payment Card Industry Secure Software Lifecycle (PCI SSLC) course provides guidelines for designing, developing, and maintaining secure software through secure governance, engineering, software and data management, and communications.

While these guidelines are provided by the payment card industry, PCI SSLC provides a strong baseline of secure development for all software.

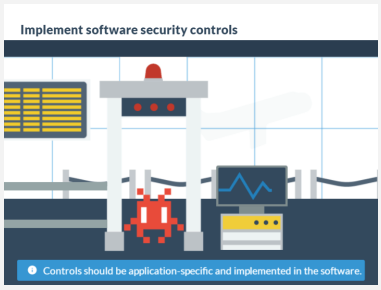
Audience

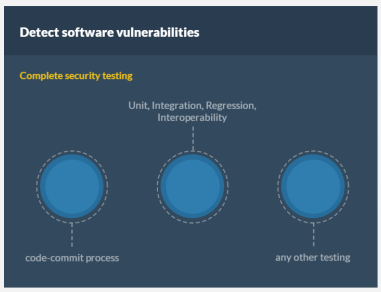
Developers

Architects

Time Required

Tailored learning - 40 minutes total





PCI102 - PCI SECURE SOFTWARE LIFECYCLE

Course Outline

1. Software security governance

- Security responsibility and resources
- Assign overall software security responsibilities by senior leadership
- Define and assign software security roles and responsibilities
- Software security policy and strategy
- Identify regulatory and compliance requirements
- Define a software security policy
- Establish a formal software security strategy
- Implement software security assurance processes
- Generate evidence for the effectiveness of assurance processes
- Monitor the effectiveness of assurance processes

2. Secure software engineering

- Threat identification and mitigation
- Identify and classify critical assets
- Identify, assess, and monitor software threats
- Implement software security controls
- Monitor and maintain software security controls
- Vulnerability detection and mitigation
- Detect software vulnerabilities
- Fix vulnerabilities

3. Secure software and data management

- Change management
- Identify, assess, approve, and track changes
- Software integrity protection
- Maintain integrity of software code and components
- Deliver software updates securely
- Sensitive data protection
- Limit the collection of production data
- Protect production data

4. Security communications

- Security guidance
- Provide stakeholders with comprehensive security guidance
- Stakeholder communications
- Establish a two-way communication channel for security issues
- Deliver security notifications and instructions to mitigate risks
- Update information
- Provide a change summary and details of impact for software updates

SecurityCompass