PCI103 – PCI Software Security Framework

Course Learning Objectives

This course covers the Payment Card Industry Software Security Framework (PCI SSF) in seven modules. By the end of this course, you'll be able to describe:

- The structure of the framework and its key components.
- Three controls for minimizing the attack surface of applications: asset identification, secure defaults, and sensitive data retention.
- The four key controls to protect the integrity and confidentiality of critical assets: critical Asset Protection, Authentication and Access Controls, Sensitive Data Protection, and Cryptography.
- The two controls for tracking activity involving critical assets: activity tracking and attack detection controls.
- The three controls that implement secure software lifecycle management practices: threat and vulnerability management, secure software updates, and software vendor implementation.
- The two controls for assessing and protecting account data that is stored, processed, and transmitted: cardholder data protection and sensitive authentication data protection.
- The five controls for protecting software intended for deployment and developing software intended for Point-of-Interaction devices: documenting, designing, mitigating attacks, security testing, and securely implementing terminal software.

Description

This course examines the PCI SSF and the PCI Security Software Standard (PCI SSS or S3), which is a component of PCI SSF. The framework was designed by the PCI Council to encourage developers to design and implement more secure software and will replace the Payment Application Data Security Standard (PA DSS) in 2022.

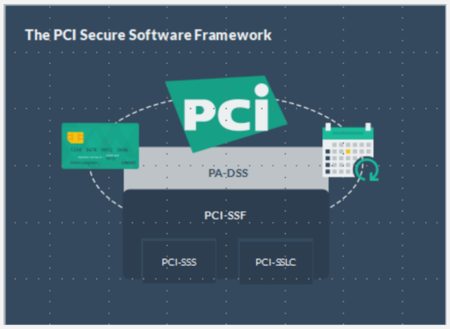
Audience

Developers, DevOps, PMs

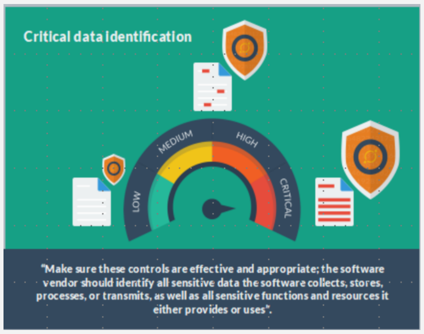
PCI Assessors

Time Required

Tailored learning - 55 minutes total approx.

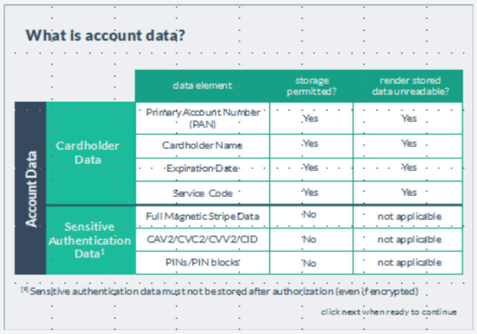


The PCI Secure Software Framework



Critical data identification

"Make sure these controls are effective and appropriate; the software vendor should identify all sensitive data the software collects, stores, processes, or transmits, as well as all sensitive functions and resources it either provides or uses".



What is account data?

		data element	storage permitted?	render stored data unreadable?
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	Yes
		Expiration Date	Yes	Yes
		Service Code	Yes	Yes
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data	No	not applicable
		CAV2/CVC2/CVV2/CID	No	not applicable
		PINs/PIN blocks	No	not applicable

[1] Sensitive authentication data must not be stored after authorization (even if encrypted)

click next when ready to continue

PCI103 – PCI Software Security Framework

Course Outline

1. Introduction to PCI SSS

- The PCi Secure Software Framework
- Relationship with PA-DSS
- Transition timelines
- Introduction to the Secure SLC Program
- SSF Assessors

2. Minimizing the attack surface

- Critical data identification
- Critical function and resource identification
- Critical asset identification
- Minimizing exposed software functions
- Limiting software privileges and resources
- Limiting default privileges for built-in accounts
- Reducing sensitive and transient data
- Securely deleting sensitive and transient data
- Minimizing data leaks

3. Software protection mechanisms

- Critical data identification
- Authentication and access control
- Protecting sensitive data
- Using cryptography

4. Secure software operations

- Tracking software activity
- What if a security control fails?
- Detecting attacks

5. Implementing SSLC

- Threat and vulnerability management
- Secure software updates
- Software implementation guidance

6. Account data

- What is account data?
- Protecting account data
- Protecting PAN data
- Protecting sensitive authentication data

Security Compass

PCI103 – PCI Software Security Framework

Course Outline

7. Terminal software

- Terminal software documentation
- Use of native functions and cryptography
- Digitally signing software files
- Prompt files
- Input validation and buffer overflows
- Unhandled exceptions
- Race conditions
- Software implementation guidance

SecurityCompass