RSI | Datasheet

PCI Software Security Framework

The Security Standards Council (SSC) of the Payment Card Industry (PCI) develops multiple frameworks to ensure the security of all stakeholders in the payment ecosystem—organizations, their staff, and their clientele. Until October 2022, the primary framework regulating payment processing software was the Payment Application Data Security Standard (PA-DSS). But moving into 2023 and beyond, it has been replaced by the Software Security Framework (SSF).

The SSF is complex, comprising two Standards and over 22 Core Objectives.

The best way to ensure SSF compliance is to work with a quality PCI SSF advisor, whose service offerings will streamline your implementation, management, and assessment of controls.

PCI SSF Security Standards

The two standards that make up the PCI SSF are the Secure Software Standard and the Secure Software Lifecycle (Secure SLC) Standard. The former applies primarily to the software itself, and vendors bear the brunt of the regulatory burden. The latter applies to the entire design process, and both development and maintenance teams may need to comply.

Each Standard comprises a series of Core Requirements, which are called Control Objectives:

Secure Software Standard Control Objectives

- Identify critical assets
- Secure default options
- Retain sensitive data
- Protect critical assets
- Control authentication and access
- Protect all sensitive data
- Use cryptographic controls

  Track relevant activity
- Detect incoming attacks
- Manage threats and vulnerabilities
- Maintain secure software updates
- Provide guidance for implementation

Secure SLC Standard Control Objectives

- Define stakeholder responsibilities
- Implement policies and strategies
- Identify and mitigate threats
- Detect and mitigate vulnerabilities
- Manage changes
- Protect integrity
- Protect sensitive data
- Provide guidance for vendors
- Communicate with stakeholders
- Provide information about updates

These Control Objectives are organized under core functions in each respective standard.

In order to be more flexible, the Secure Software Standard also adds 11 additional Control Objectives organized under separate Modules. Currently, there are three of these modules:

Module A – Applicable to Account Data protection on most applications

Module B – Applicable to applications that run on terminals

Module C – Applicable to applications that are considered web software

Benefits of PCI SSF Advisory

By working with a PCI SSF Advisor, you can swiftly identify which SSF standards apply to your software (and which additional Modules of the Secure Software Standard may apply). Then, you can work closely with the advisor to identify gaps between your current applications and development processes and the suite of controls required by the SSF. Most importantly, your advisor will optimize these compliance practices, minimizing your overall security spend while maximizing your cyberdefense posture.

PCI SSF Advisory Services

RSI Security offers a suite of PCI SSF Advisory services, encompassing all elements of compliance. We assist with preparation, certification, and long-term maintenance through:

General SSF Scope Review

Work with an advisor to understand what apps or development processes are in scope for compliance and how to optimize the assessment.

Security Software Standard Gap Analysis

Identify and mitigate gaps between Security Software Standard requirements and the applicable applications your organization manages.

Secure SLC Standard Gap Analysis

Assess readiness and needs for remediation with respect to the Secure SLC Standard requirements and software development processes.

Depending on your organization's security maturity and compliance needs for PCI SSF, DSS, and other regulations, you may benefit from a specific service or a combination of services.

Benefits of PCI SSF Advisory

If your organization is a vendor or developer of payment processing software, you likely need to ensure that the apps or their development processes are secure. If you are both a vendor and developer, you may need to assure security across both. Compliance can be extremely challenging given the complexity and the possibility of overlap with controls from other applicable regulations.

Working with a quality SSF Advisor will streamline your PCI SSF compliance.

About RSI Security

RSI Security has provided PCI advisory and assessment services to countless organizations, for DSS, PA-DSS, SSF, and other forms of compliance. Our experts have helped secure cardholder data (CHD) and other protected categories of information from security risks for over a decade. We are recognized by the SSC as an Approved Scanning Vendor (ASV) and Qualified Security Assessor (QSA); we can assist with all elements of PCI compliance, from preparation through certification.

Working with RSI Security, you'll rethink and optimize your PCI SSF compliance.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com