RSI | *Whitepaper*

What are the Nuances Around SSF?

858.999.3030 | info@rsisecurity.com
2023

TABLE OF CONTENTS

Payment Card Industry (PCI) Security Standards Council (SSC)

1. What is the PCI SSF?
2. What Does SSF Compliance Entail?
3. The Secure Software and Secure SLC Standards
4. Which Organizations Need SSF Advisory?
5. The Benefits of SSF Advisory
6. Broader PCI Compliance Advisory

What is the PCI SSF?

The Payment Card Industry (PCI) Security Standards Council (SSC) launched the Software Security Framework (SSF) in late 2022. It replaced the Payment Application Data Security Standard (PA-DSS), and it prescribes security requirements for payment software. It applies to developers and vendors of payment apps, safeguarding operations to protect financial data.

PCI SSF compliance is a system of cybersecurity implementation and assessment that ensures any cardholder data (CHD) that comes into contact with payment applications is secure.

What Does SSF Compliance Entail?

The SSF is a regulatory framework. It stipulates requirements organizations need to meet by installing controls and assessing their performance. Like all PCI frameworks, it comprises:

Standards

The SSF comprises two distinct security standards (see below), which break down into respective sets of Objectives and controls required to meet them.

Documentation

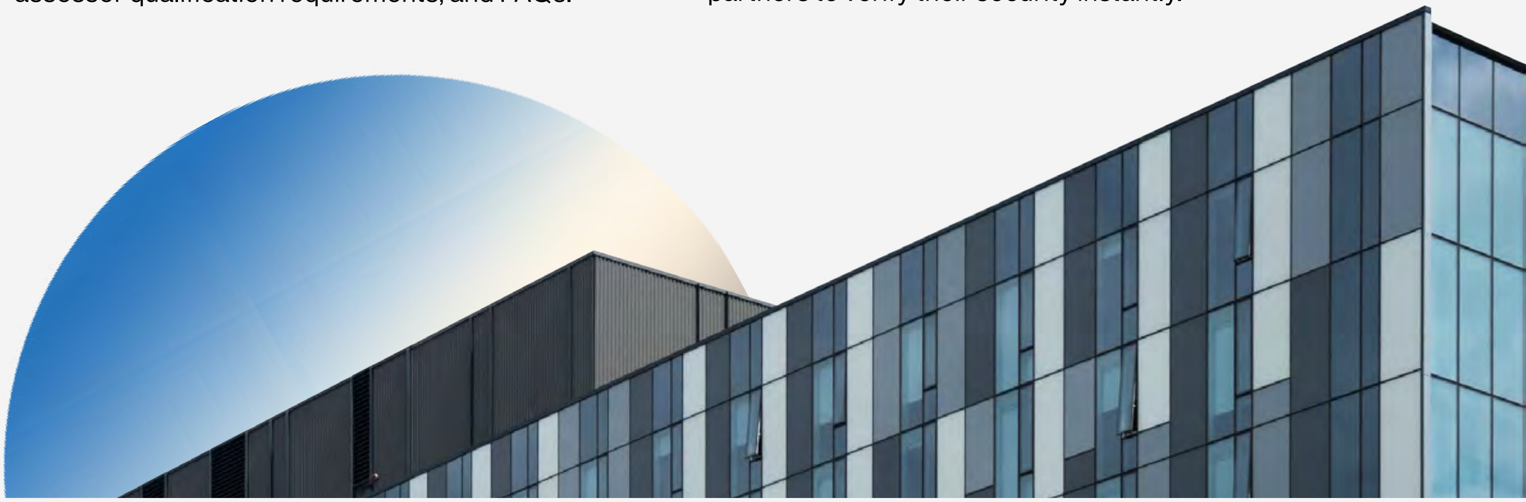
The PCI SSC offers several resources to support organizations' compliance, like the PCI SF Glossary, assessor qualification requirements, and FAQs.

Validation

There are formal processes for assessing an organization's security infrastructure, including specific reporting protocols, available in the Program Guide.

Listings

After passing audits, compliant applications and vendors are listed by the SSC on their website, allowing clients and partners to verify their security instantly.



The Secure Software and Secure SLC Standards

Unlike some more straightforward regulations, the SSF comprises two unique standards: the Secure Software Standard and the Secure Software Lifecycle (Secure SLC) Standard. Each document has a unique set of Core Requirements, which break down into Control Objectives.

The Secure Software Standard’s Requirements and Objectives	The Secure SLC Standard’s Requirements and Objectives
Minimizing Attack Surfaces 1. Identify critical assets 2. Secure default options 3. Retain sensitive data	**Software Security Governance** 1. Define stakeholder responsibilities 2. Implement policies and strategies
Software Protection Mechanisms 4. Protect critical assets 5. Control authentication and access 6. Protect all sensitive data 7. Use cryptographic controls	**Secure Software Engineering** 3. Identify and mitigate threats 4. Detect and mitigate vulnerabilities
Secure Software Operations 8. Track relevant activity 9. Detect incoming attacks	**Secure Software and Data Management** 5. Manage changes 6. Protect integrity 7. Protect sensitive data
Secure Software Lifecycle Management 10. Manage threats and vulnerabilities 11. Maintain secure software updates 12. Provide guidance for implementation	**Security Communications** 8. Provide guidance for vendors 9. Communicate with stakeholders 10. Provide information about updates

All Objectives break down further into Test Requirements, which specify the conditions that need to be satisfied, and Guidance, which provides reasoning and support for meeting them.

Which Organizations Need SSF Advisory?

The Secure Software Standard applies primarily to software vendors, and the Secure SLC Standard applies to developers. Collectively, the SSF applies to all organizations that are involved in creating, distributing, and managing payment applications, especially—

PA-DSS software

Applications that were previously subject to PA-DSS Requirements (and their developers and vendors) are now required to meet the new SSF Objectives.

Qualified payment apps

The Secure Software Standard includes extra Modules and Objectives for specific kinds of software, like terminal and web applications. At present, the Core Requirements and Module A Requirements apply to almost all applications.

Developers of payment apps

Organizations involved in developing one or more payment apps need to ensure uniform security protections across the lifecycles of each.

Any organizations engaged in development related to payment applications should consider SSF implementation. It establishes public credibility and may be required now or in the future.

The Benefits of SSF Advisory

The SSF enhances security across all use cases and environments for payment software. It aligns directly with the development and deployment of apps, rather than broader network security that impacts them indirectly. It's more focused than the PA-DSS, enabling precise assessments, and its flexibility affords clients and end-users greater clarity regarding the specific protections implemented and auditing methodologies used to verify them.

PCI SSF advisory enables organizations to reap these benefits more efficiently.

The Secure Software and Secure SLC Standards

The PCI SSF is one of many regulatory frameworks overseen by the SSC to protect CHD. Depending on your organization's size, payment processing infrastructure, and relationship to CHD, you may need to comply with multiple overlapping standards simultaneously.

Consider these other frameworks and implications for PCI compliance:

The Data Security Standard (DSS)

The DSS ensures network security for all organizations that store or process CHD.

Point-to-Point Encryption (P2PE)

P2PE applies to encryption solutions for storing or transmitting CHD.

Mobile Payments on COTS (MPoC)

MPoC protects CHD across both software-based and contactless solutions.

PIN Transaction Security (PTS)

PTS and Point of Interaction (POI) Requirements prevent physical threats to CHD.

Three Domain Security Standard (3DS)

PCI's 3-D security protects CHD in e-commerce and related contexts.

Approved Scanning Vendor (ASV)

Depending on organization size, verified audits may need to be conducted by an ASV.

PCI Compliance with RSI Security

RSI Security is committed to helping organizations achieve and maintain PCI compliance. Our advisors will work with your team to scope, strategize, and implement SSF, DSS, and other framework controls. We'll conduct readiness and gap assessments to ensure that you're prepared for verification. And, as an ASV, we'll help you audit and verify your security.

Work with RSI Security to rethink your compliance and streamline CHD protections.