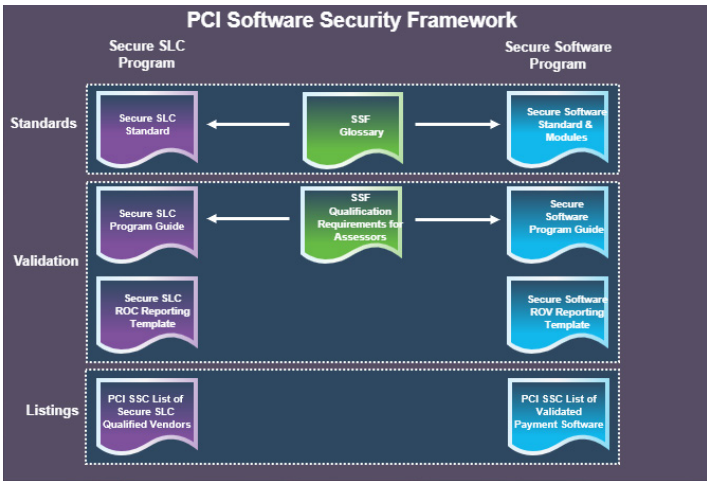
PCI Software Security Framework Provides a Modern Approach to Payment Software Security

The PCI Software Security Framework (SSF) is a collection of standards and programs for the secure design and development of payment software. Security of payment software is a crucial part of the payment transaction flow and is essential to facilitate reliable and accurate payment transactions. The SSF replaces the Payment Application Data Security Standard (PA-DSS) with modern requirements that support a broader array of payment software types, technologies, and development methodologies. With its outcome-focused requirements, the SSF provides more agility for developers to incorporate payment application security with nimble development practices and frequent update cycles. The SSF enables accelerated provision of customization and features for payment applications for merchants without compromising security. It also improves consistency and transparency in testing payment applications, which elevates the validation assurance for merchants, service providers, and acquirers that implement and manage the use of payment solutions. This At-a-Glance provides an overview and describes the significance of the SSF, its benefits for payments industry stakeholders, and how it is used.



Framework Benefits

- Provides new approach for validating security of traditional, modern, and future payment software
- Promotes developer education on the importance of integrating security into the software development lifecycle
- Supports nimble software development processes and methodologies
- Offers flexibility for Secure SLC Qualified Vendors to manage delta changes for Validated Payment Software
- Provides authoritative lists of Validated Payment Software and Secure SLC Qualified Vendors on the PCI SSC website

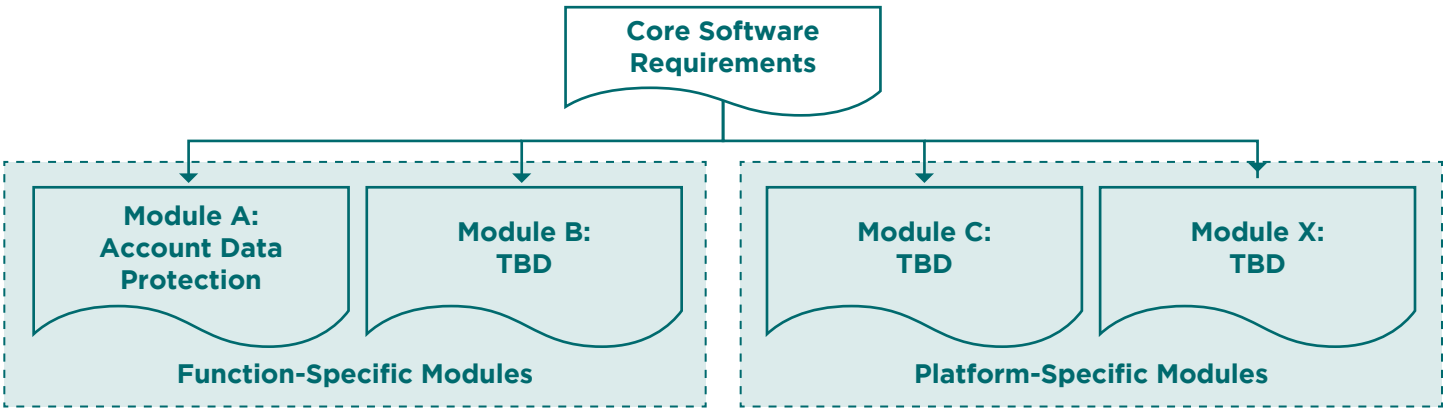
Flexible Requirements and Validation Options Support Broader Range of Payment Software

Modern software development requires objective-focused security to support more nimble development and update cycles than traditional software development practices. The PCI Software Security Framework (SSF) recognizes this evolution with an approach that supports both traditional and modern payment software. It provides a new methodology for validating software security and a separate secure software lifecycle qualification for vendors with robust security development practices.

The SSF works in a similar manner to the PA-DSS program. Secure Software Framework Assessors (SSF Assessors) evaluate vendors and their payment software products against the Secure Software Lifecycle (Secure SLC) Standard and the Secure Software Standard, respectively. The PCI SSC lists both Secure SLC Qualified Vendors and Validated Payment Software on the Council's website as resources for merchants, service providers, and acquirers. As new modules are added to the Secure Software Standard to address other types of software, use cases, and technologies, the program scope will expand to support them.

PCI Security Standards Council®

Secure Software Standard



Conceptually, the module-based architecture of the Secure Software Standard is composed of core software requirements for payment software, supported by function and platform-specific modules to address particular use cases. Validation procedures are prescribed by associated Programs for the Secure Software Standard and the Secure Software SLC Standard, which are followed by SSF Assessors.

Secure Software Standard

The Secure Software Standard provides security requirements for building secure payment software to protect the integrity and the confidentiality of sensitive data that is stored, processed, or transmitted in association with payment transactions. It is intended for vendors that develop payment software that supports or facilitates payment transactions.

Secure Software Program

Validation to the Secure Software Standard shows that the payment software product is designed, engineered, developed, and maintained in a manner that protects payment transactions and data, minimizes vulnerabilities, and defends against attacks.

Upon successful evaluation by a Secure Software Assessor, validated payment software will be recognized on the PCI SSC List of Validated Payment Software, which will supersede the current List of Validated Payment Applications when PA-DSS is retired the end of October 2022. Until then, PCI SSC will continue to maintain the PA-DSS Program and list, which includes honoring existing validation expiration dates until the end of October 2022, and accepting new PA-DSS submissions through 30 June 2021.

Secure Software Lifecyle (Secure SLC) Standard

The Secure SLC Standard provides security requirements for payment software vendors to integrate security throughout the entire software lifecycle, which results in software that is secure by design and able to withstand attacks. It is intended for vendors that are developing payment software that supports or facilitates payment transactions.

Secure SLC Program

Validation to the Secure SLC Standard illustrates that the software vendor has secure software lifecycle management practices in place to ensure its payment software is designed, developed, and maintained to protect payment transactions and data, minimize vulnerabilities, and defend against attacks.

Upon successful validation by a Secure SLC Assessor, software vendors will be recognized on the PCI SSC List of Secure SLC Qualified Vendors. They will be able to self-attest to delta changes for any of their products listed as Validated Payment Software under the Secure Software Program and developed using the validated SLC process.

Software Security Framework Assessors (SSF Assessors)

PCI SSC qualifies companies and individuals within those companies to perform SSF assessments. SSF Assessor Company qualification is open to any company that meets the qualification requirements. Companies can qualify to perform Secure SLC assessments, Secure Software assessments, or both. In order to be listed as an SSF Assessor Company on the PCI SSC website, the company must have at least one employee successfully complete the Secure Software Assessor or Secure SLC Assessor training and exam. For additional information, refer to the Software Security Framework - Qualification Requirements for Assessors.

For specific information and resources to assist with migration to SSF from PA-DSS, refer to this PCI SSC Resource Guide: Transitioning from PA-DSS to the PCI Software Security Framework.

PCI Security Standards Council