SecurityCompass

New PCI Software Security Framework: How Will Your Organization Comply?

Security Compass supports PCI compliance in modern development environments.

On January 16th, 2019, the PCI Security Standards Council (SSC) released new PCI Software Security Standards which have raised the bar for software security. These new standards mandate that payment software be secure by design–that is, built to protect the integrity of payment transactions and the confidentiality of sensitive data. They are presented in 3 components:

- The **Secure Software Requirements and Assessment Procedures** or the **Secure Software Standard**: *A rigorous standard that relies on in-depth security testing techniques to validate whether a software release is compliant*.

- The **Secure Software Lifecycle (Secure SLC or SSLC) Requirements and Assessment Procedures** or the **Secure SLC Standard**: *An optional standard that assesses security throughout the software development and operations lifecycle. By complying with the Secure SLC requirements, organizations can forgo the need to have each release assessed by a qualified assessor, enabling better modern agile and continuous delivery software practices.*

Mid-year 2019, the PCI SSC expects to release the third component in the software security framework, called the '**Validation Program**.' This is a program for software vendors to validate how they can properly manage the security of payment software throughout the entire software lifecycle.

Who Will Be Affected?

Initially, the new standards will affect vendors or providers of Payment Applications (PA), rather than those companies that procure and deploy PA for their e-commerce needs. Payment processor companies have historically been subject to compliance with the Payment Application Data Security Standard (PA-DSS), and the new standards are an extension of this, now more prescriptive about how the software is secured. The new standards have been written so that they can be referenced by other PCI standards in the future. Anyone who participates in the credit card ecosystem, including merchants, should take note of these changes.

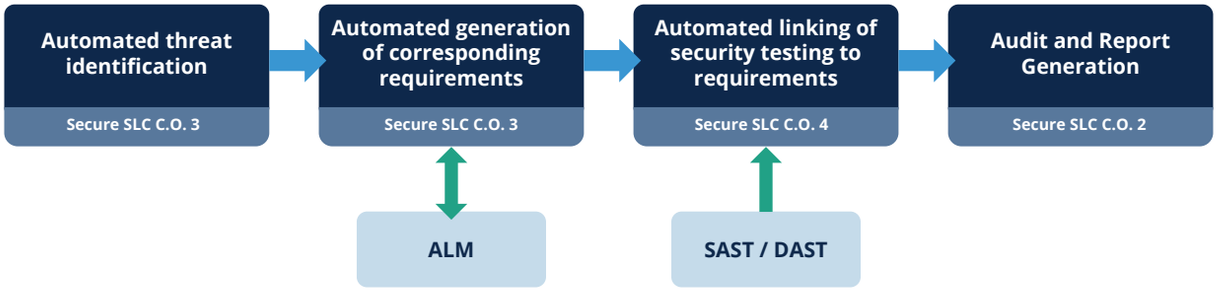
How Will The New Standards Impact Your Organization?

There is an enhanced focus on implementing a secure software development process for Payment Applications. PA providers will be obliged to drastically improve their application security programs in order to comply. This may also apply to other payment ecosystem participants in the future. Thus, PA providers will need to transform their organizational secure development practices. Unlike previous PCI standards, the Software Security Standards are objective-based, thus offering vendors flexibility in how they go about complying with each specific objective.

Our Solution: How We Can Help You Comply

POLICY-TO-PROCEDURE PLATFORM

The new standards require the implementation of secure development practices, which involves manual activities that slow down business. SD Elements is the most comprehensive software solution for compliance with the PCI Software Security Standards' software development standards. It helps enterprises by automating the secure development process, end-to-end. Just by using SD Elements, organizations can easily implement industry standard frameworks' application security processes, such as ISO 27034. SD Elements offers automated threat modeling and requirements generation, allowing you to comply with Control Objective 3 at the speed of modern development. These requirements integrate with the automated security testing tools, satisfying the traceability requirement in Objective 4. Its extensive reporting capabilities, including the verification of controls, allow easy demonstration of compliance in the event of an audit.



JUST-IN-TIME TRAINING SOFTWARE

Our unique market offering, Just-in-Time Training (JITT), provides secure coding guidance for developers, delivering task-specific instructions at the point of need. We also provide standard eLearning courses designed to train clients in security practices required by the new PCI Software Security Standards, including threat modeling, application security testing, and more.

IMPLEMENTATION SERVICES

We offer a proven implementation methodology to ensure the successful adoption of our software. Working together with your team, we help develop processes and integrate tools, so that you can meet the new PCI compliance standards in a cost-effective manner.

VERIFICATION SERVICES

Our verification services help to identify vulnerabilities, commensurate with the PCI Software Security Standard Control Objectives. We offer penetration testing, red teaming, vulnerability triaging for Static and Dynamic Application Security Testing tools, and more. Our security consultants have extensive experience with enterprise clients, fixing and breaking code while taking a strategic approach to your organization's security problems. We can also help you prepare for a successful security requirement audit.

Examples of PCI Secure Software Lifecycle Requirements Control Objectives Addressed by Security Compass Solution

Control Objective 1: Security Responsibility and Resources	▸ Just-in-Time training provides secure coding guidance to developers. ▸ We developed a software security policy template which offers guidance on how to comply with the new PCI standards. This template can easily be used and customized for your organization's unique work environment. The template offers guidance by outlining and defining roles & responsibilities as they relate to software security.
Control Objective 2: Software Security Policy and Strategy	▸ SD Elements provides all necessary compliance requirements for your software's development. It automatically generates all of the tasks your developers need to complete to ensure that your software is secure and compliant. These tasks can easily be understood and acted upon by your developers. ▸ SD Elements automatically generates reports which clearly communicate the compliance status of your software. ▸ SD Elements provides testing and process tasks related to software assurance, with corresponding reports. The testing tasks instruct you on how to test your software and the process tasks instruct you on security practices surrounding secure development.
Control Objective 3: Threat Identification and Mitigation	▸ SD Elements' risk policies set a high standard for the qualifying as a "completed" or "verified" PCI-related control status. ▸ SD Elements generates a report that details all threats applicable to a project as well as the status of the controls used to mitigate these threats. ▸ SD Elements can be used to create process tasks that will help your team maintain an inventory of open source components. These tasks also ensure that vulnerabilities in your open source components are tracked and patched.
Control Objective 4: Vulnerability Detection and Mitigation	▸ SD Elements integrates with Static & Dynamic Analysis Security Testing (SAST & DAST) tools to track and verify PCI security control requirements. ▸ SD Elements features task verification statuses for security controls. ▸ SD Elements automatically generates reports that clearly show a list of verification statuses. These lists are generated in SD Elements through input from integrated tools or manual testing.

SD Elements can be used to create and track 'Process Tasks,' to guide organizations through the compliance process from Control Objectives 1 – 10. Security Compass is actively working on new training material to educate users on how to implement these Process Tasks. Our combined offering, consisting of SD Elements, training, and these upcoming materials, is the most comprehensive on the market, allowing organizations to cost-effectively achieve compliance with the new PCI Software Security Standards.

For a more detailed review of the new PCI Software Security Standards and information on how our solution addresses all Control Objectives, access the full guide at www.securitycompass.com/pci/ or contact us at info@securitycompass.com

securitycompass.com
twitter.com/securitycompass
linkedin.com/company/security-compass

Security Compass