Service Description

Secure Software Lifecycle Standard

Compliance Validation Service

Contents

Secure Software Lifecycle Standard Compliance Validation Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Secure Software Lifecycle Standard Compliance Validation Service (Secure SLC CVS) is a professional services engagement. The Secure SLC CVS is designed to validate if an organization has implemented software lifecycle (SLC) management practices, security operations and controls in accordance with the Payment Card Industry (PCI) Software Security Framework (SSF) Secure SLC Standard compliance objectives. The Secure SLC CVS is an evaluation of the design and implementation of SLC management practices, controls and supporting policies and procedures relevant to the PCI SSF Secure SLC Standard requirements, assessment procedures and the SLC under review.

BASE SERVICE FEATURES

The SecureTrust Secure SLC CVS includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

Global Compliance and Risk Services

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Security Consultant – An information security consultant and SSF Assessor who is the primary resource for the fulfilment of the service, responsible for conducting the assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and reporting quality assurance to the Security Consultant and serves as a secondary point of contact for escalations and queries.

Compliance Review Board (CRB) – The CRB serves as an escalation point for requirement interpretation or complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is the final point of escalation for issue resolution regarding compliance status against requirement interpretation or the review of a compensating control.

Secure SLC CVS – An assessment to validate whether Client's SLC management practices, security operations and controls have achieved the PCI SSF Secure SLC Standard compliance objectives. If Client's SLC management practices under review are found compliant with the PCI SSF Secure SLC Standard compliance objectives, SecureTrust will provide a Report on Compliance (ROC) as a declaration of the compliance status. If Client is found non-compliant with the PCI SSF Secure SLC Standard compliance objectives, SecureTrust will provide a non-compliant ROC.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the service which includes scheduling and conducting the remote kickoff meeting to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures.

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of the SLC.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information about the SLC. SecureTrust will conduct interviews, as required, with system architects, application developers, database developers, system administrators, quality assurance (QA), testing personnel and other Client personnel who may provide relevant details on the SLC.

SecureTrust will examine applicable documentation and may request additional information and examples from Client in order for the Security Consultant to gain a clear picture of the SLC design and capabilities.

Topics for information gathering include, but are not limited to, the following:

- Description of the SLC to provide a fundamental understanding of the SLC to the assessor and for inclusion in the report deliverable;
- Description of the components/functions that make up the SLC;
- List of any third-party dependencies required by the SLC as well as a list of development tools used during design, code development and software integration, as applicable;
- Key management operations including any integrations with any third-party encryption functions, as applicable;
- SLC flow diagrams and documentation illustrating the SLC’s process flow;
- List of testing tools that may be required for lab testing, description of SLC test environment documentation for data processing, as applicable; and
- Details of testing and SLC evaluation lab location and requirements.

Phase II: Secure SLC Validation

The Secure SLC Validation will take place predominantly within Client’s premises. Some aspects of the assessment may be carried out remotely. SecureTrust will work with Client to determine the requirements which require an onsite visit and which requirements and testing procedures can be completed remotely.

SecureTrust will review the SLC’s functions, including end-to-end software development processes, software security policies and strategies, software engineering, vulnerability and change management, software integrity control, sensitive data protection mechanisms, the assessment also includes review of the vendor security guidance, the stakeholder communication methods and software update mechanisms, as applicable. SecureTrust will review documentation accuracy, including external customer documentation and accuracy of internal documentation to the SLC's functionality and implementation processes.

The results of the SLC evaluation will provide a detailed report on the SLC processes and any remediation steps required for the SLC to be deemed compliant with the Secure SLC Standard requirements.

Phase III: Reporting

SecureTrust will develop a compliant or a non-compliant Secure SLC ROC, depending on the status of the SLC processes at the time the validation occurs.

Report deliverables will be sent to Client for review. Client will be able to comment and suggest changes to the final deliverable and supporting documentation before SecureTrust's QA group finalizes the report.

Report deliverables will be submitted to the SecureTrust QA team for review.

SecureTrust will provide a final deliverable, as defined below:

- If the SLC is found compliant with the Secure SLC Standard requirements, once finalized by SecureTrust's QA group, the ROC, Attestation of Compliance (AOC) together with required supporting documentation, will be submitted to the PCI Security Standards Council (SSC) for listing consideration.
- If the SLC is found to be non-compliant with the Secure SLC Standard requirements, SecureTrust will provide Client with a non-compliant ROC.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with Client.
- Establish communication and escalation plans.
- Create a Client account in the SecureTrust Portal.
- Define high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Validate the scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform validation in accordance with the Secure SLC Standard testing procedures.
- Provide Client with information on any findings that requires remediation.
- Determine Secure SLC Validation results and compliance status at the end of the Secure SLC Validation process.
- Produce either a compliant or a non-compliant Secure SLC ROC, depending on the status of the SLC processes at the time the validation occurs.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with SecureTrust.
- Establish communication and escalation plans.

- Agree to high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable client environment information and configuration requirements.
- Inform SecureTrust of all Client environment maintenance activity and changes that may impact the service.
- Accurately respond to requests from SecureTrust when establishing contact and collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in compliance assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - SecureTrust's Secure SLC CVS uses the requirements and testing procedures of the current Secure SLC Standard version applicable at the time of the service start date.
    - The engagement consists of both remote and onsite assessment activities.
    - The Secure SLC validation process will begin on the day of the kickoff call. The timeline and end of the Secure SLC validation process will be determined during the kickoff call.
    - Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the Secure SLC validation process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Secure SLC validation process.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant findings, and one review of the Client remediated documentation.
    - The Secure SLC validation process includes one SLC evaluation and does not include retesting of findings that, once remediated, require onsite validation services.
        - For remediation items that can be validated remotely, one remediation cycle following the initial SLC evaluation is included.
    - Test environment preparations are the responsibility of Client. Client must provide an environment that is appropriate for testing against all of the PCI Secure SLC requirements.
    - SecureTrust may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
    - SecureTrust is not responsible for defining systems in scope or whether information provided by Client is accurate.
    - SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the service.
    - SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.
    - SecureTrust will perform the service in the English language.
    - SecureTrust will not create or modify Client documentation as part of the Secure SLC CVS.

- SecureTrust will not provide remediation services as part of the Secure SLC CVS.
- SecureTrust will not offer any legal guidance or counseling.
- The quality and accuracy of the service is dependent on Client’s provision of accurate information and access to Client systems and resources to SecureTrust.
- Pricing excludes the PCI SSC listing fee, payable per application deemed compliant and listed directly to the PCI SSC.