SecureTrust
a Trustwave division

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 (SLC) Compliance Validation Service (CVS) (the "**Service**") is designed to validate whether Client's software lifecycle (SLC) management practices, security operations, and controls are compliant with the Payment Card Industry (PCI) Software Security Framework (SSF) Secure SLC Standard.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between SecureTrust and Client.

BASE SERVICE FEATURES

The Service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal features consist of, among others, 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:

SSF Assessor – An SSF Assessor is Client's primary resource during the Service and is responsible for conducting the assessment, determining compliance, and drafting reports.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the SSF Assessor and serves as Client's secondary point of contact for escalations and queries.

Compliance Review Board (CRB) – The CRB serves as a final escalation point for interpreting the requirements of the PCI SSF Secure SLC standard or resolving complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is also the final point of escalation for issue resolution regarding compliance status against the requirements of the PCI SSF Secure SLC standard or the review of a compensating control.

Secure SLC CVS – SecureTrust determines whether Client's SLC management practices, security operations, and controls are compliant with the PCI SSF Secure SLC standard. If Client's SLC management practices are found compliant with the PCI SSF Secure SLC standard, SecureTrust will provide Client with a Report on Compliance (ROC) as a declaration of Client's compliant status. If Client

is found non-compliant with the PCI SSF Secure SLC Standard compliance objectives, SecureTrust will provide Client with a non-compliant ROC.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by 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 Client's SLC.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information about Client's 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 have relevant details.

SecureTrust will examine applicable documentation and may request a remote demonstration of Client's SLC capabilities to understand Client's SLC.

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

- Description of Client's SLC;
- Description of the components/functions that make up Client's SLC;
- List of any third-party dependencies for Client's SLC and development tools used during design, code development, and software integration, as applicable;
- Key management operations including any integrations with third-party encryption functions, as applicable;
- SLC flow diagrams and documentation illustrating Client's SLC's process flow;
- List of testing tools that may be required for lab testing, description of Client's 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

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, controls analysis and examination of Client's current security architecture.

The Secure SLC Validation will take place primarily onsite within Client's facilities. Some aspects of testing may be carried out remotely, as determined by SecureTrust.

SecureTrust will examine Client's SLC according to applicable PCI SSF Secure SLC standard security requirements in place as of the Service start date.

Where third parties are used to support Client's SLC, SecureTrust may collect information about the services provided by and the relationships with such third parties.

SecureTrust will work with Client to determine the testing requirements for each control objective of the Service.

SecureTrust will review Client's SLC's functions, including:

- end-to-end software development processes
- software security policies and strategies
- software engineering, vulnerability and change management processes
- software integrity controls, and sensitive data protection mechanisms

SecureTrust will review Client's vendor security guidance, stakeholder communication methods, and software update mechanisms, as applicable. SecureTrust will review the accuracy of Client's SLC documentation, including external customer facing documentation and internal documentation of Client's SLC's functionality and implementation processes.

When sampling is permitted by the PCI SSF Secure SLC standard testing procedures, SecureTrust may utilize non-statistical (non-random) sampling, also known as judgement sampling, to determine the population and the sample.

Compensating controls may be considered, at SecureTrust's sole discretion when Client cannot meet a PCI SSF Secure SLC standard requirement explicitly as stated due to legitimate technical or documented business constraints if SecureTrust determines that Client has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

SecureTrust will work with Client to resolve Client's assessment questions. SecureTrust will also provide the Client reasonable assistance in Client's interpretation of the PCI SSF Secure SLC standard and its responses. SecureTrust may request additional review of Client's SLC, documentation, or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a draft report documenting observations and recommendations from the Service.

The draft report will be sent to Client for review. Client may comment and suggest changes to the draft report with supporting documentation. SecureTrust retains final authority regarding the contents of the final report and the type of deliverables to be produced.

SecureTrust will provide a final deliverable, as defined below:

- If Client's SLC is found compliant with the PCI SSF Secure SLC standard, the ROC, Attestation of Compliance (AOC), and required supporting documentation will be submitted to the PCI Security Standards Council (SSC) for listing consideration.
- If Client's SLC is found to be non-compliant with the PCI SSF Secure SLC standard, SecureTrust will provide Client with a non-compliant ROC.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from 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 Secure SLC CVS.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform Secure SLC CVS in accordance with the PCI SSF Secure SLC standard.
- Identify to Client observations that may require remediation.
- Determine Service results and compliance status at the end of the Service.
- Produce either a compliant or a non-compliant ROC, depending on the status of Client's SLC at the time the Service occurs.
- Deliver to Client a final report documenting all observations and recommendations from the Service.

CLIENT RESPONSIBILITIES

- Establish contact and remain available for communications from 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 the Service 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.
    - The Service uses the requirements and testing procedures of the current PCI SSF Secure sLC Standard version applicable at the time of the Service start date.
    - The Service may consist of both remote and onsite assessment activities.
    - The Service will begin on the day of the kickoff call. The timeline and end of the Service 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 Service.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Service.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant observations and one review of the Client remediated documentation.

- The Service includes one SLC evaluation and does not include retesting of observations 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 SSF Secure SLC standard 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 Service.
- SecureTrust will not provide remediation services as part of the Service.
- 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.