SecureTrust
a Trustwave division

Service Description

Software Security Framework Pre-Assessment Workshop

Contents

Software Security Framework Pre-Assessment Workshop

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Software Security Framework (SSF) Pre-Assessment Workshop (the "**Service**") is a high-level overview of compliance with the Payment Card Industry (PCI) SSF standards, via an evaluation of security requirements as required by such PCI SSF standards.

SecureTrust will evaluate policies, procedures, and practices through documentation review, interviews, discussions, and review of Client's current security architecture.

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 workshop, evaluating compliance, and producing reports.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the P2PE QSA as well as serves as a secondary point of contact for escalations and queries.

Compliance Review Board (CRB) – The CRB serves as a final point for interpreting the requirements of the PCI SSF standards 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 standards or the review of a compensating control.

SSF Pre-Assessment Workshop – SecureTrust aims to identify high-level gaps and helps prioritize areas that may require immediate remediation to achieve compliance with the PCI SSF standards. A SSF

Assessor will provide Client with a high-level analysis of Client's existing PCI SSF security operations and safeguards through a series of workshops and consulting.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by scheduling and conducting a 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.

The SSF Assessor will work with Client and provide high-level pre-assessment consulting activities related to the following standards:

- PCI SSF – Secure Software Lifecycle (SLC) Standard
- PCI SSF – Secure Software Standard

SecureTrust may request documents and schedule future meetings. Client will provide a preliminary overview of Client's SLC and software.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's SLC and software.

SecureTrust will examine applicable design documentation to understand Client's secure SLC processes Secure Software, and design parameters. Topics for information gathering may include, but are not limited to, the following:

- Focus areas of the Secure SLC requirements
- Focus areas of the Secure Software requirements
- Third parties supporting Client's SLC or software

Phase II: Workshop

The Workshop phase may take place onsite within the Client's facilities or may be carried out remotely. A SSF Assessor will work with Client to determine the high-level review requirements for each of the SSF standards, as applicable.

Workshop activities may include:

- Interviews;
- Physical inspection of facilities and equipment;
- Review of SLC and software design and architecture; and
- High level review of applicable PCI SSF requirements.

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

The Service is not intended to focus on any specific controls. The goal of the Service is to make a determination of Client's ability to undergo a Secure SLC or Secure Software Standard validation and to, where possible, identify suggested priority areas for remediation.

Phase III: Reporting

SecureTrust will develop a high-level draft report that outlines areas of concern in relation to each SSF standard, as applicable.

The draft report will be sent to Client for review. Client may comment on and suggest changes to the draft report before finalization. SecureTrust retains final authority regarding the contents of the final report and the type of deliverable to be produced.

SecureTrust will provide an final report as the final deliverable.

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, workshop, and closeout meetings.
- Interview appropriate Client personnel and collect information from personnel.
- Identify to Client observations that may require remediation.
- Produce final report.
- Deliver to Client a final report documenting 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 teams when establishing contact and collection of required 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 is designed to provide high-level pre-assessment consulting activities related to the following standards:
        - PCI SSF – Secure SLC Standard
        - PCI SSF – Secure Software Standard

- SecureTrust uses the requirements and testing procedures of the current Secure Software or Secure SLC standard version applicable at the time of the Service start date.
- The Service does not include in-depth testing or review of system settings, configurations, or observation of implemented processes and procedures.
- The Service does not include visits to third parties used to support the SLC and software under review.
- The Service does not include detailed evaluation against the SSF controls for the SLC and software under review.
- 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.
- The Service may consist of both onsite and remote assessment activities.
- 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.