SecureTrust
a Trustwave division

Service Description

Software Security Framework General Consulting

Contents

Software Security Framework General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Software Security Framework (SSF) General Consulting (the "**Service**") is consulting for solution design, application design, policies, procedures, and practices employed, or intended for use, by Client to comply with the Payment Card Industry (PCI) SSF standards.

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 scheduling and conducting consulting activities.

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

Compliance Review Board (CRB) – The CRB serves as a final point for interpreting 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 General Consulting – An SSF Assessor provides general consulting on requirement interpretation, compliance challenges, solution or application design, policies, procedures and other subjects related to the PCI SSF standards. The SSF Assessor analyzes Client's existing or planned PCI SSF security operations and safeguards through onsite or remote consulting.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the SSF General Consulting 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.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's SSF environment.

SecureTrust will examine applicable design documentation to understand Client's SSF environment's functionality, data handling processes, and design parameters.

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

- Critical assets;
- Business processes;
- Security and compliance management processes in place; and
- Previous compliance or assessment documentation.

Phase II: SSF General Consulting

The Service may take place onsite within Client's facilities or delivered remotely, at SecureTrust's discretion. A SecureTrust SSF Assessor will work with Client to determine the areas of the PCI SSF standards on which to focus.

- SecureTrust will provide consulting on areas agreed between SecureTrust and Client and which relate to Client's SSF environment. SecureTrust will provide the Service according to the PCI SSF standards the following standards: PCI SSF – Secure Software Lifecycle (SLC) Standard
- PCI SSF – Secure Software Standard

The Service may include, but are not limited to, the following:

- Review of policies and procedures
- Examination of system configurations
- Interviews
- Observation of processes and procedures actually performed in accordance with documentation collected during the Information Gathering phase
- Physical inspection of facilities and equipment
- Identification and high-level review of third parties used to virtually support Client's PCI PIN environment
- Guidance on specific questions from Client regarding PCI SSF requirements

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

The Service is not intended to focus on any specific controls, unless explicitly agreed between SecureTrust and Client. The purpose of the Service is to assist Client in determining better courses of action for PCI SSF focus areas, to assist Client in making a determination of Client's ability to undergo a SSF security assessment, and, where possible, to identify suggested priority areas for remediation. The Service is not a replacement for a PCI SSF compliance report nor should be treated as such.

Phase III: Reporting

The Service does not include any report deliverable. It is an hourly consulting service.

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 key steps, estimates for duration, and resource requirements.
- Schedule and conduct kickoff, periodic status, and closeout meetings.
- Interview applicable Client personnel and collect information from such personnel.
- Provide Client with feedback on observations identified during the SSF General Consulting that may require remediation.

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.
- 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 standards applicable at the time of the Service start date.
    - The Service is designed to provide general consulting for the requirements related to the following standards:
        - PCI SSF – Secure SLC Standard

        - PCI SSF – Secure Software Standard
    - The Service does not include any report deliverable. It is an hourly consulting service offered.
    - 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 onsite visits to third parties used to support Client's SSF environment.
    - The Service may consist of remote consulting 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 will perform the Service in the English language.
    - 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.