SecureTrust
a Trustwave division

Service Description

Software Security Framework Consulting

Contents

Software Security Framework Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Software Security Framework (SSF) Consulting is a professional services engagement. The SSF Consulting is offered as general consulting for subjects related to compliance with the Payment Card Industry (PCI) SSF. The SSF Consulting service involves consulting for solution design, application design, policies, procedures, and practices employed, or intended for use, by organizations to meet applicable SSF compliance objectives.

BASE SERVICE FEATURES

SecureTrust's SSF Consulting 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 is the primary resource for the fulfilment of the service, responsible for conducting the service.

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.

SecureTrust 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.

SSF Consulting – Services to assist Client with general consulting for requirement interpretation, compliance challenges, solution or application design, policies, procedures and any other subject related to the PCI SSF. SSF Consulting provides assistance in analyzing Client's existing or planned PCI SSF security operations and safeguards through onsite and/or remote consulting, as needed.

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.

General Consulting

The SecureTrust Security Consultant will work with Client and provide general consulting, guidance and recommendations to achieve and maintain compliance with the PCI SSF standards:

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

SSF General Consulting activities may include, but are not limited to the following:

- Help clients understand PCI SSF compliance requirements;
- Prepare and coach clients;
- Advise clients in preparation of the payment software environment;
- Review and provide guidance for PCI SSF scoping documentation;
- Review and provide guidance for the design and implementation of PCI SSF security controls;
- Advise clients of any compliance gaps identified;
- Help clients prioritize remediation actions to achieve and maintain PCI SSF compliance; and
- Provide recommendations for remediation of PCI SSF compliance issues.

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with Client.
- Establish communication and escalation plans.
- Define high-level project plan consisting of key steps, estimates for duration, and resource requirements.
- Schedule and conduct SSF Consulting activities.

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 consulting 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 SSF Consulting 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
    - SecureTrust's SSF Consulting service does not include any report deliverable, it is an hourly consulting service offered as consulting at Client's discretion.
    - SecureTrust's SSF Consulting service consists 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 create or modify Client documentation as part of the SSF Consulting.
    - SecureTrust will not provide remediation services as part of the SSF Consulting.
    - 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.