

Service Description

Software Security Framework Pre-Assessment Workshop

Contents

Software Security Framework Pre-Assessment Workshop	3
Service Description	3
Base Service Features	3
SecureTrust Portal.....	3
Global Compliance and Risk Services	3
Delivery and Implementation.....	4
Project Initiation	4
Phase I: Onsite / Remote Information Gathering	4
Phase II: Pre-Assessment Workshop.....	4
Phase III: Reporting.....	5
SECURETRUST RESPONSIBILITIES	5
CLIENT RESPONSIBILITIES.....	5

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 is a professional services engagement. The SSF Pre-Assessment Workshop is a high-level overview of compliance with the Payment Card Industry (PCI) SSF standards, via an evaluation of security requirements as required by the SSF standards. The SSF Pre-Assessment Workshop involves various policies, procedures and practices that will be evaluated by SecureTrust through interviews, documentation review and review of an organizations current security architecture.

BASE SERVICE FEATURES

SecureTrust's SSF Pre-Assessment Workshop 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 Pre-Assessment – An assessment to identify high-level gaps and prioritize areas that may require immediate remediation to achieve compliance with the PCI SSF standards. The SSF Pre-Assessment Workshop provides a high-level analysis of Client's existing PCI SSF security operations and safeguards through a series of workshops and/or consulting.

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.

The SecureTrust security consultant 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 will request initial information documents and schedule future meetings. Client will provide a preliminary overview of the software/SLC under review.

Phase I: Onsite / Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on the software/SLC under review.

SecureTrust will examine applicable design documentation to maximize the understanding of the secure SLC processes and/or Secure Software, and design parameters, before conducting the SSF Pre-Assessment Workshop. 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
- Identification of third parties supporting the SLC/Software

Phase II: Pre-Assessment Workshop

The SSF Pre-Assessment Workshop will take place primarily within the Client's facilities. However, some aspects of the assessment may be able to be carried out remotely. A SecureTrust security consultant will work with Client to determine the high-level review requirements for each of the SSF standards, as applicable.

SecureTrust will work with client to perform a high level evaluation of the SLC/software under review according to applicable SSF requirements, discussing testing requirements and their applicability to the software under review.

Example pre-assessment workshop activities may include:

- Interviews;
- Review of SLC/Software design/architecture
- High level review of applicable SSF requirements.

SecureTrust will work with Client to identify and if possible, resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional information on the functions of the SLC/Software under review.

The pre-assessment workshop is not intended to focus on any specific controls, unless explicitly requested by Client. The goal of the pre-assessment workshop is to make a determination of Client's

ability to undergo a Secure SLC or Secure Software Standard validation and identify areas of prioritization for remediation, where possible.

Phase III: Reporting

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

The report will be sent to Client for review. Client will be able to comment on and suggest changes to the report before finalization.

SecureTrust will provide an executive summary report as the final deliverable.

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, workshop and closeout meetings.
- Interview appropriate organization personnel and collect information from personnel.
- Conduct the SSF Pre-Assessment Workshop.
- Provide Client with information on any findings that requires remediation.
- Produce executive summary report.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the pre-assessment workshop.

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 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 workshop 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 Pre-Assessment Workshop 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 SSF Pre-Assessment Workshop does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
- The SSF Pre-Assessment Workshop does not include visits to third parties used to support the SLC/Software under review.
- The SSF Pre-Assessment Workshop does not include detailed evaluation against the SSF controls for the SLC/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 assessment consists 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 SSF Pre-Assessment Workshop.
- SecureTrust will not provide remediation services as part of the SSF Pre-Assessment Workshop.
- 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.