SecureTrust
a Trustwave division

Service Description

Software Security Framework Gap Assessment

Contents

Software Security Framework Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Software Security Framework (SSF) Gap Assessment is a professional services engagement. The SSF Gap Assessment helps to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the Payment Card Industry (PCI) SSF standards. The SSF Gap Assessment provides an analysis of PCI SSF security operations and safeguards. The SSF Gap Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection and an overview of an organization's current security architecture.

BASE SERVICE FEATURES

SecureTrust's SSF Gap Assessment 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 assessment, compliance determination and reporting.

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 Gap Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the PCI SSF standards. SecureTrust will provide Client with an SSF Gap Assessment. SecureTrust will provide a report detailing the results of the SSF Gap Assessment.

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 to provide a gap assessment between current secure operations and the requirements related to one of 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 SLC/Software under review.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on the SLC/Software under review. SecureTrust will conduct interviews, as required, with solution architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and other Client personnel who may provide relevant details of the SLC/Software under review.

SecureTrust will examine applicable design documentation to maximize understanding of the SLC/Software, and design parameters, before conducting the SSF Gap Assessment portion of the assessment.

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

- Identification if a current vendor release agreement is on file with the PCI SSC;
- Determination of third parties used to support the SLC/Software;
- Review of SLC/Software processes;
- Collection and review of applicable documentation;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Security Guidance review;

Phase II: Gap Assessment

The SSF Gap Assessment will take place primarily within the Client's facilities. Some aspects of the assessment may be able to be carried out remotely. A SecureTrust security consultant will work with Client to determine the review requirements for the SSF standard, as applicable.

SecureTrust will examine the SLC/Software according to all applicable SSF requirements. Example testing activities may include:

- Observation of the practical implementation of policies, processes and procedures;
- Interviews;
- Identification of third parties used to support the SLC/Software
- Examination of implemented secure software controls.

The gap assessment is not intended to perform a full laboratory test of the SLC/Software under review.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional review of documentation or reviews of processes and procedures.

Phase III: Reporting

SecureTrust will develop an SSF Gap Assessment Report document to identify any areas of non-compliance pertaining to the SSF standards. Included in the SSF Gap Assessment Report are all non-compliant requirements, identified threats, vulnerabilities or potential vulnerabilities. Wherever possible, the report recommends specific changes that may be required to bring Client's SLC/Software into compliance with the SSF standards.

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

SecureTrust will provide an SSF Gap Assessment 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, periodic status and closeout meetings.
- Validate the scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform gap assessment against the requirements and testing procedures of the current Software Security Standard or Secure SLC Standard version applicable at the time of the service start date .
- Determine SSF gap assessment results and the SLC/Software compliance status.
- Produce an SSF gap assessment report based on the status of the SLC/Software at the time the gap assessment occurs.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

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 collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in compliance assessment 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 Gap Assessment will, unless specifically requested by client, provide a gap assessment between current secure operations and the requirements related to one of the following standards:
        - PCI SSF – Secure SLC Standard
        - PCI SSF – Secure Software Standard
    - 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's SSF Gap Assessment 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.
    - SecureTrust's SSF Gap Assessment consists of both remote and onsite assessment activities.
    - SecureTrust's SSF Gap Assessment process will begin on the day of the kickoff call. The timeline and termination of the SSF Gap Assessment process 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 SSF Gap Assessment process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the SSF Gap Assessment process.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant findings, and one review of the Client remediated documentation.
    - SecureTrust's SSF Gap Assessment does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - SecureTrust's SSF Gap Assessment does not include visits to third parties used to support the SLC/Software under review.
    - 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 Gap Assessment.

- SecureTrust will not provide remediation services as part of the SSF Gap Assessment.
- 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.