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 (the "**Service**") is deigned 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.

SecureTrust evaluates policies, procedures, and practices through documentation review, interviews, facilities inspections, controls analysis, and examination 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 assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the CPSA 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 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 Gap Assessment – SecureTrust aims to identify gaps and helps prioritize areas that may require remediation to achieve compliance with the PCI SSF standards. SecureTrust will provide a report detailing the results of the assessment.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by 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 kickoff meeting also aims to verify the applicable PCI SSF standards. The following PCI standards are defined by the PCI Security Standards Council (SSC):

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

The Service may cover one or both PCI SSF standards (to be agreed during scoping).

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

Phase I: Information Gathering

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

SecureTrust will examine applicable design documentation and may request a remote demonstration of Client's SLC/Software to maximize understanding of Client's 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:

- Whether a current vendor release agreement is on file with the PCI SSC;
- Third parties used to support Client's SLC and software;
- SLC and software processes;
- Applicable documentation;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Security Guidance review;

Phase II: Assessment

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, controls analysis, and examination of Client's current security architecture.

The Assessment phase may take place onsite within Client's facilities or may be carried out remotely, to be determined by SecureTrust.

SecureTrust will examine Client's SLC and software according to applicable SSF Security standards.

Where third parties are used to support Client's SLC and software, SecureTrust may collect information about the services provided and the relationships with such third parties.

A SSF Assessor will work with Client to determine the testing requirements for each area of Client's SLC and software. Example testing activities may include:

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

The Service is not intended as a full laboratory test of Client's SLC and software.

When sampling is permitted by the PCI SSF testing procedures, SecureTrust may utilize non-statistical (non-random) sampling, also known as judgement sampling, to determine the population and the sample.

SecureTrust will identify areas of non-compliance to Client's primary point of contact.

Compensating controls may be considered, at SecureTrust's sole discretion, when an entity cannot meet a PCI SSF Security standard as stated due to legitimate technical or documented business constraints provided that SecureTrust determines that the Client has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

SecureTrust will work with Client to resolve Client's assessment 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 SLC and software, applicable code areas, documentation or data handling processes and procedures. SecureTrust may request additional review of Client's SLC and software, documentation, or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop an SSF Gap Assessment Report documenting observations and recommendations from the SSF Gap Assessment. The SSF Gap Assessment Report includes details of non-compliant observations and recommends specific changes that may be required to bring Client's SLC and software into compliance with the PCI SSF standards.

The draft SSF Gap Assessment Report will be sent to Client for review. Client may comment and suggest changes to the draft report. SecureTrust retains final authority regarding the contents of the final SSF Gap Assessment Report

SecureTrust will provide a final SSF Gap Assessment Report.

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, periodic status, and closeout meetings.
- Validate the scope of the Service.
- Respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform the Service against the requirements and testing procedures of the current Software Security Standard or Secure SLC Standard applicable at the time of the Service start date .
- Provide Client with information on any observations that require remediation.

- Determine assessment results and Client's SLC and software compliance status.
- Produce a draft SSF Gap Assessment Report.
- Deliver to Client a final SSF Gap Assessment 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 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 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 will include, unless specifically requested by Client, a gap assessment of current secure operations as compared to 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.
    - The Service 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 may consist of both remote and onsite assessment activities.
    - The Service will begin on the day of the kickoff call. The timeline and termination of the Service 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 Service.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Service.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant observations, and one review of the Client remediated documentation.
    - 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.
- 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.