SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard

Gap Assessment

Contents

PCI DSS Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Gap Assessment (the "Service") is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the PCI DSS as set out by the PCI Security Standards Council (the "Standard").

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:

Qualified Security Assessor (QSA) – A QSA is the primary resource for the fulfilment of the Service, responsible for performing the assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the QSA as well as 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 Standard 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 Standard or the review of a compensating control.

Gap Assessment – The assessment identifies gaps and prioritizes areas that may require remediation to achieve compliance with the Standard. SecureTrust will provide Client with guidance for design of PCI DSS controls and identification of supporting organizational policy, procedures, and practices relevant to the Standard. SecureTrust will provide Client with a final report detailing the results of the Service.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates 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.

Phase I: Information Gathering

SecureTrust and Client will work together to gather and analyze information about Client's in scope systems.

SecureTrust will work with Client, where applicable, to:

- Determine critical assets;
- Examine business processes;
- Identify security and compliance management processes in place; and
- Review previous PCI DSS compliance documentation.

Phase II: PCI DSS Gap Assessment

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

SecureTrust will work with Client, where applicable, to:

- Assess adequacy of Client knowledge about the Standard and responsibilities of all parties involved to demonstrate PCI DSS compliance;
- Gain an understanding of the environment to identify critical gaps between Client's current state and the Standard;
- Gain an understanding of Client's PCI DSS compliance posture;
- Identify gaps to achieve compliance with the Standard; and
- Prioritize remediation efforts required to achieve compliance with the Standard.

SecureTrust will analyze evidence in accordance with the Standard and determine the compliance status of Client's in scope systems.

Phase III: Reporting

SecureTrust will develop a report documenting observations and recommendations from the Service.

A draft report will be sent to Client for review. Client will be able to comment and suggest changes to the draft report before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

SecureTrust will provide Client with a final report as the final deliverable.

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 scope of the Service, including segmentation, and discuss sampling methodology.
- Create and respond to Client action items within the Compliance Manager Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform gap assessment against the Standard testing procedures.
- Determine Service results and in accordance with the Standard.
- Produce a draft report at the time the assessment occurs.
- Deliver to Client a final report documenting all observations and recommendations from the assessment.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- 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 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 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 not take the place of a PCI DSS compliance validation assessment and will not result in a report on compliance or an attestation of compliance.
    - The Service may consist of both remote and onsite assessment activities.
    - The project start and end dates will be determined during the kickoff call.
    - 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 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 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.