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 is a professional services engagement. The PCI DSS Gap Assessment is designed to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the PCI DSS.

BASE SERVICE FEATURES

SecureTrust's PCI DSS 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:

Qualified Security Assessor (QSA) – An information security consultant and QSA is the primary resource for the fulfilment of the service, responsible for performing the compliance assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight and reporting quality assurance to the QSA 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.

Gap Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the PCI DSS. SecureTrust will provide guidance for design of PCI DSS controls and identification of supporting organizational policy, procedures and practices relevant to PCI DSS. SecureTrust will provide a gap assessment report.

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.

Phase I: Discovery

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.

SecureTrust will begin report deliverable development.

Phase II: PCI DSS Gap Assessment

SecureTrust will work with Client, through interviews, discussions, and facilities inspections to:

- Assess adequacy of Client knowledge about PCI DSS requirements 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 PCI DSS requirements;
- Gain an understanding of Client PCI DSS compliance posture;
- Identify gaps to achieve compliance with the PCI DSS; and
- Prioritize remediation efforts required to achieve compliance with the PCI DSS.

SecureTrust will continue development of the report deliverable.

Phase III: Reporting

SecureTrust will analyze evidence in accordance with the PCI DSS, determine Client compliance status and complete development of the report deliverable.

SecureTrust will deliver the final report deliverable to Client point of contact and/or relevant reporting entities, summarizing the current state of Client's PCI DSS compliance.

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 scope of the engagement, 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.
- Determine gap assessment results and in accordance with the PCI DSS.
- 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 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 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.
    - The PCI DSS Gap Assessment 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 consists of both remote and onsite assessment activities.
    - The service period 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 PCI DSS Gap Assessment.
    - SecureTrust will not provide remediation services as part of the PCI DSS 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.