SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard

Self-Assessment Consulting

Contents

PCI DSS – Self-Assessment Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Consulting service is a subscription service. SecureTrust's PCI DSS Self-Assessment Consulting service includes access to external vulnerability scanning (EVS) and the PCI Manager applications as well as professional services to aid organizations in completion of their self-assessment questionnaire (SAQ) as part of the compliance validation process.

BASE SERVICE FEATURES

SecureTrust's PCI DSS Self-Assessment Consulting service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among others, the following key applications and functions:

External Vulnerability Scanning (EVS) – Unlimited EVS during the term producing reports with a high-level summary for executives and managers as well as detailed results and general remediation guidance for technicians. Remediation guidance includes Common Vulnerability and Exposures (CVE) linked vulnerability checks and best practices defined by SecureTrust.

PCI Manager – An easy-to-use tool to assist merchants and service providers in completion of a PCI SAQ to satisfy reporting requirements of acquirers and the card brands.

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, who will conduct the remote consulting portion of the engagement.

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.

Remote Consulting – Directed guidance to help Client complete a PCI SAQ.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to help facilitate delivery of the service which includes remotely creating an instance for the Client within the SecureTrust Portal, and 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: PCI Manager Online Questionnaire and External Vulnerability Scanning

SecureTrust's PCI Manager provides an easy-to-use tool to assist merchants and service providers in completion of a PCI SAQ, with self-help and a continuously updated FAQ database, to satisfy reporting requirements of the card associations. The questionnaire is available in English (American and British), French, Canadian French, Swedish, Greek, Spanish, Japanese, Chinese (Simplified and Traditional).

Unlimited External Vulnerability Scanning (EVS) is available during the term. Through a secure web interface, Client may schedule scans producing concise, auto-generated reports with a high-level summary for executives and managers as well as detailed results and general remediation guidance for technicians. Remediation guidance includes common vulnerabilities and exposures (CVE) linked vulnerability checks and best practices defined by SecureTrust.

Email and multilingual phone support are available for SecureTrust applications.

Phase II: Remote Consulting

A SecureTrust security consultant will provide directed guidance to help Client reach its compliance goals within the term. A SecureTrust QSA consultant will host a series of calls throughout the term, once the initial SAQ and EVS are completed.

The purpose of the remote consulting is to:

- Identify areas of non-compliance uncovered in the questionnaire and scan results
- Provide scope reduction guidance
- Provide policy and procedure guidance
- Provide network security infrastructure and architecture guidance
- Provide guidance to assist in completion of Client's self-assessment

Phase III: Documentation of Results

The appropriate SAQ will be generated to document the results of the Client's self-assessment of compliance with the PCI DSS requirements which will include the identification of any non-compliant findings.

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 and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.

CLIENT RESPONSIBILITIES

- Establish communication and escalation plans.
- Establish and maintain contact with SecureTrust.
- 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 when establishing contact and collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available Client resources capable of participating 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 service is a remote engagement.
    - 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 Self-Assessment Consulting service.
    - SecureTrust will not provide remediation services as part of the PCI DSS Self-Assessment Consulting 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.