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 (the "Service") that includes professional consulting services and access to the SecureTrust Portal applications to aid organizations in completing their Payment Card Industry (PCI) self-assessment questionnaire (SAQ) and managing their PCI external vulnerability scans to help 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, the following key applications and functions:

PCI Manager, PCI Scanning – This application to manages unlimited PCI external vulnerability scans with an approved scanning vendor (ASV) certified scanner, and generates PCI ASV scan reports.

PCI Manager, SAQ Wizard – An easy-to-use SAQ Wizard tool to assist Client 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) – A QSA is the primary resource for the fulfilment of the Service and is responsible for scheduling and conducting consulting activities.

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

PCI DSS Self-Assessment Consulting – Consulting and guidance to help Client complete a PCI SAQ.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates 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 SAQ Wizard and PCI Scanning

SecureTrust's PCI Manager provides an easy-to-use SAQ Wizard tool to assist Client in completion of a PCI SAQ 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).

SecureTrust's PCI Manager provides unlimited PCI external vulnerability scans during the term of the Service.

Email and multilingual phone support are available for SecureTrust Portal applications.

Phase II: PCI DSS Self-Assessment Consulting

SecureTrust's QSA and Client will work together to review and examine requirements to achieve and maintain compliance with the Standard. The Service activities may include, but are not limited to, the following:

- Identify areas of non-compliance;
- Provide scope reduction guidance;
- Provide policy and procedure guidance;
- Provide network security infrastructure and architecture guidance; and
- Provide guidance to assist in completion of Client's PCI DSS compliance self-assessment.

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

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- Establish contact and remain available for communications from 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 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 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 in the English language.
    - 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.