SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard

Remediation Service

Contents

PCI DSS Remediation Service 3
Service Description 3
Base Service features 3
SecureTrust Portal 3
Global Compliance & Risk Services 3
Delivery and implementation 3
Project Initiation 3
Phase I: Remote Consulting Engagement 4
SECURETRUST RESPONSIBILITIES 4
CLIENT RESPONSIBILITIES 4

PCI DSS Remediation Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Remediation Service is a professional services engagement. PCI DSS Remediation Service consulting is designed to assist and guide organizations in achieving and maintaining compliance with the PCI DSS.

BASE SERVICE FEATURES

SecureTrust's PCI DSS Remediation Service 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 & 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 and is responsible for scheduling and conducting consulting activities.

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.

PCI DSS Remediation Consulting – Remote consulting and guidance for achieving and maintaining compliance with the PCI DSS. SecureTrust will work with Client to develop prioritized action plans and processes for remediation.

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, resource requirements and escalation procedures.

Phase I: Remote Consulting Engagement

SecureTrust's information security consultant will work with Client and provide guidance and recommendations to create prioritized action plans and target processes for remediation. Remediation service activities may include working with Client to:

- Create a remediation action plan for ineffective controls
- Design processes and projects to remediate known gaps for high priority and high risk areas
- Leverage common controls across Client's control environment to remediate identified gaps
- Determine evidence and documentation needed to demonstrate compliance
- Identify Client's key challenges and risks associated with achieving PCI DSS compliance
- Establish self-assessment procedures to be executed by control owners for high priority areas

SecureTrust will conduct a closeout meeting with Client, if desired.

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 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 consulting 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 consists of remote consulting.
    - 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 assessment.
- SecureTrust will perform the service 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.