SecureTrust
a Trustwave division

Service Description

Payment Card Industry Three Domain Secure (PCI 3DS) General Consulting

Contents

PCI 3DS General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Three Domain Secure (PCI 3DS) General Consulting (the "**Service**") is consulting for solution design, application design, policies, procedures and practices employed, or intended for use, by organizations to comply with the PCI 3DS standards set out by the PCI Security Standards Council (SSC) (the "**PCI 3DS 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 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 PCI 3DS 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 PCI 3DS standard or the review of a compensating control.

PCI 3DS General Consulting – A SecureTrust QSA assists and guides Client with general consulting for PCI 3DS requirement interpretation, compliance challenges, solution or application design, policies, procedures, and any other subject related to the PCI 3DS standard. The QSA aids in analyzing Client's existing or planned PCI 3DS security operations and safeguards through onsite or remote consulting, at SecureTrust's sole discretion.

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.

The kickoff meeting also aims to verify Client's PCI 3DS function. The following PCI 3DS functions are defined by the PCI SSC:

- 3DS Server (3DSS)
- 3DS Directory Server (DS)
- 3DS Access Control Server (ACS)

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of Client's PCI 3DS data environment.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on the PCI 3DS data environment.

SecureTrust will examine applicable documentation and may request from Client a remote demonstration of the PCI 3DS data environment capabilities to maximize understanding of the data handling processes and design parameters before conducting the Service.

Topics for information gathering include, but are not limited to, the following:

- Policies and procedures
- Key management
- Configuration standards
- Vulnerability management
- Access control
- Media management
- Incident response
- System development life cycle (SDLC)
- Security governance
- Data management
- Risk management

Phase II: General Consulting

The Service may take place within the Client's facilities, or it may be delivered remotely, at SecureTrust's discretion. A SecureTrust QSA will work with Client to determine the areas of the PCI 3DS standard on which to focus the Service.

SecureTrust will provide consulting around areas agreed by SecureTrust and Client and which relate to Client's PCI 3DS data environment. Consulting will be delivered according to the PCI 3DS standard, discussing testing requirements and their applicability to Client's environment.

Example consulting activities may include:

- Review of policies and procedures
- Examination of system configurations
- Interviews
- Observation of performed processes and procedures in accordance with documentation collected during the Information Gathering phase
- Physical inspection of facilities and equipment
- Identification and high-level review of third parties used to support Client's PCI 3DS data environment
- Consulting on specific PCI 3DS requirements.

SecureTrust will work with Client to resolve Client's assessment questions. SecureTrust will also provide Client reasonable assistance in Client's interpretation of the PCI 3DS standard and its responses. SecureTrust may request additional review of Client's PCI 3DS data environment, documentation, or data handling processes and procedures.

The Service is not intended to focus on any specific controls, unless explicitly agreed to by Client and SecureTrust. The purpose of the Service is to assist Client in determining the best course of action for PCI 3DS focus areas, and assist Client in making a determination of Client's ability to undergo a PCI 3DS security assessment, and, where possible, to identify suggested priority areas for remediation. The Service is not a replacement for a PCI 3DS compliance report nor should be treated as such.

Phase III: Reporting

The Service does not include any report deliverable, it is an hourly consulting service.

SecureTrust will conduct a closeout meeting with Client when Client has clearly communicated an end to the Service.

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.
- Interview appropriate organization personnel and collect information from personnel.
- Provide Client with feedback on any observations identified during the Service that may require remediation.

CLIENT RESPONSIBILITIES

- 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 collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available 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 uses the requirements and testing procedures of the current PCI 3DS standard version applicable at the time of the Service start date.
    - The Service does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - The Service does not include visits to third parties used to support the PCI 3DS data environment.
    - The Service may consist of onsite and remote assessment activities.
    - 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.
    - All PCI services selected for a single SOW or Order Form must be for an identical term.
    - 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 provide remediation services as part of 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.