SecureTrust
a Trustwave division

Service Description

Payment Application Data Security Standard General Consulting

Contents

PA-DSS General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Application Data Security Standard (PA-DSS) General Consulting (the "**Service**") is consulting for solution design, application design, policies, procedures and practices employed, or intended for use, by organizations to meet applicable PA-DSS controls as set forth by the PCI Security Standards Council (PCI SSC) (the "**PA-DSS"**).

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:

Payment Application Qualified Security Assessor (PA QSA) – A PA 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 PA QSA as well as 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 PA-DSS 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 PA-DSS or the review of a compensating control.

PA-DSS General Consulting – A SecureTrust PA QSA assists Client with general consulting for requirement interpretation, compliance challenges, solution or application design, policies, procedures and any other subject related to the PA-DSS. SecureTrust will provide Client with assistance in analyzing Client's existing or planned PA-DSS security operations and safeguards through onsite and/or remote consulting, as determined by SecureTrust.

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.

SecureTrust will request initial information and schedule future meetings. Client will provide a preliminary overview of Client's PA-DSS solution, component or application.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information about Client's PA-DSS solution, component or application. SecureTrust will conduct interviews, as required, with system architects, application developers, database developers, system administrators, quality assurance (QA) or testing personnel and other Client personnel who may provide relevant details on the application.

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

- Description of the application to provide a fundamental understanding of Client's application;
- Description of the components that make up Client's application;
- List of hardware and software required to run Client's application, including any third-party dependencies, as applicable;
- Description of Client's application's role in the payment lifecycle, including authorization and settlement functions, as applicable;
- Software Development Lifecycle (SDLC) processes; and
- Functional design specifications showing Client's application design and functional implementations.

Phase II: PA-DSS General Consulting

The Service may take place within the Client's facilities, or it may be delivered remotely, as determined by SecureTrust. A SecureTrust PA QSA will work with Client to determine the areas of the PA-DSS on which to focus the Service, as applicable.

SecureTrust will provide the Service around areas chosen by Client that relate to the PA-DSS and the Service will be delivered according to the applicable PA-DSS requirements, discussing testing requirements and their applicability to Client's solution, component or application.

Example consulting activities may include:

- Interviews;
- Identification of use of third-party support for Client's PA-DSS solution, component or application, and a high-level assessment of the PCI DSS and PA-DSS compliance of those third parties, if applicable; and
- Consulting on specific PA-DSS requirements.

SecureTrust will work with Client to identify and if possible, resolve Client's assessment questions and SecureTrust will provide Client reasonable assistance in Client's interpretation of the PA-DSS and its responses. SecureTrust may request additional review of Client's PA-DSS solution, component or application, documentation, or process and procedures.

The Service is not intended to focus on any specific controls, unless explicitly requested by Client. The goal of the Service is to assist Client in determining the best course of action for any PA-DSS focus areas chosen by Client, and assist Client in making a determination of Client's ability to undergo a PA-DSS validation, and to, where possible, identify suggested priority areas for remediation.

Phase III: Reporting

The Service does not include any report deliverable, it is an hourly consulting service offered as consulting at Client's discretion.

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.
- Interview applicable organization personnel and collect information from personnel.
- Conduct Service activities.
- Identify to Client any observations identified during the Service that may require remediation.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- 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, 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 uses the requirements and testing procedures of the current PA-DSS 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 application.

- 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 Confirmation must be for an identical term.
- The Service may consist of onsite and remote assessment activities.
- SecureTrust is not responsible for defining systems in scope or for establishing 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 Service.
- SecureTrust will not provide remediation services as part of the 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.