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 is a professional services engagement. The PA-DSS General Consulting 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.

BASE SERVICE FEATURES

SecureTrust's PA-DSS General Consulting 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 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 Payment Application Data Security Standard (PA-DSS) QSA is the primary resource for the fulfilment of the service, responsible for delivering the consulting services.

Managing Consultant (MC) – An MC provides guidance, project oversight, and quality assurance to the PA-DSS 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.

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

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 the PA-DSS solution, component or application.

Phase I: Information Gathering

SecureTrust will work with Client to gather and analyze information about the 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 the application;
- Description of the components that make up the application under review;
- List of hardware and software required to run the application, including any third-party dependencies, as applicable;
- Description of the application's role in the payment lifecycle, including authorization and settlement functions, as applicable;
- Software Development Lifecycle (SDLC) processes;
- Functional design specifications showing the application design and functional implementations;

Phase II: General Consulting

The PA-DSS General Consulting may take place within the Client's facilities, or it may be delivered remotely, at Client's discretion. A SecureTrust security consultant will work with Client to determine the areas of the PA-DSS standard on which to focus the consulting services, as applicable.

SecureTrust will provide consulting around areas chosen by Client that relates to the application. Consulting will be delivered according to the applicable PA-DSS requirements, discussing testing requirements and their applicability to the environment under review.

Example consulting activities may include:

- Interviews;
- Identification of third parties used to support the PA-DSS environment, and a high-level assessment of the PCI DSS and PCI 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 questions and assist Client in interpreting PA-DSS requirements.

The general consulting is not intended to focus on any specific controls, unless explicitly requested by Client. The goal of the general consulting 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 areas of prioritization for remediation.

Phase III: Reporting

The PA-DSS General Consulting 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 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.
- Interview applicable organization personnel and collect information from personnel.
- Conduct the PA-DSS General Consulting.
- Provide Client with feedback on any findings identified during the consulting PA-DSS General Consulting that may require remediation.

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, 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.
    - SecureTrust uses the requirements and testing procedures of the current PA-DSS version applicable at the time of the service start date.
    - The PA-DSS General Consulting does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - The PA-DSS General Consulting 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 services selected must be for an identical term.
- The service consists of onsite or remote assessment activities.
- 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 PA-DSS General Consulting.
- SecureTrust will not provide remediation services as part of PA-DSS General Consulting.
- 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.