SecureTrust
a Trustwave division

Service Description

PCI PIN General Consulting

Contents

PCI PIN General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Personal Identification Number (PCI PIN) General Consulting is a (the "**Service**") consulting for solution design, application design, policies, procedures, and practices employed, or intended for use, by organizations to comply with the PCI PIN security requirements and the Qualified PIN Assessor (QPA) Program Guide 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, 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 PIN Assessor (QPA) – A QPA 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 QPA 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 PIN version 3 Security Requirements 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 PIN General Consulting – A SecureTrust QPA offers Client general consulting on requirement interpretation, compliance challenges, solution or application design, policies, procedures, and other subjects related to the Standard. The QPA may assist in analyzing Client's existing or planned PCI PIN security operations and safeguards through onsite or remote consulting.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team initiates the Service by scheduling and conducting a 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 PCI PIN environment.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's PCI PIN environment.

SecureTrust will examine applicable design documentation to understand Client's PCI PIN environment's functionality, data handling processes, and design parameters.

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

- Determine critical assets;
- Examine business processes;
- Identify security and compliance management processes in place; and
- Review previous compliance or assessment documentation.

Phase II: PCI PIN General Consulting

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

SecureTrust will provide consulting around areas agreed between Client and SecureTrust which relate to Client's PCI PIN environment. Consulting will be delivered according to the Standard, discussing testing requirements and their applicability to Client's environment.

The Service activities may include, but are not limited, the following:

- Reviewing 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 PIN environment; and
- Consulting on specific PCI PIN 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 Standard and its responses. SecureTrust may request additional review of Client's PCI PIN environment, documentation or data handling processes and procedures.

The Service is not intended to focus on any specific controls, unless explicitly agreed between SecureTrust and Client. The purpose of the Service is to assist Client in determining the best course of

action for PCI PIN focus areas and assist Client in making a determination of Client's ability to undergo a PCI PIN security assessment, and, where possible, to identify suggested priority areas for remediation.

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.

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.
- Provide Client with feedback on 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, 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 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 Standard applicable at the time of the Service start date.
    - The Service does not include any report deliverable, it is an hourly consulting service.
    - The Services 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 Client's PCI PIN 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 PIN 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.