

Service Description

PCI PIN General Consulting

Contents

PCI PIN General Consulting	3
Service Description	3
Base Service Features	3
SecureTrust Portal.....	3
Global Compliance and Risk Services	3
Delivery and Implementation.....	4
Project Initiation	4
Phase I: Onsite / Remote Information Gathering	4
Phase II: General Consulting.....	4
Phase III: Reporting.....	5
SECURETRUST RESPONSIBILITIES	5
CLIENT RESPONSIBILITIES.....	5

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 professional services engagement. The PCI PIN General Consulting service is consulting for solution design, application design, policies, procedures and practices employed, or intended for use, by organizations to comply with the PCI PIN standard.

BASE SERVICE FEATURES

SecureTrust's PCI PIN 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 PIN Assessor (QPA) – An information security consultant and Qualified PIN Assessor (QPA) 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 QPA 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.

PCI PIN General Consulting – Services to assist Client with general consulting for requirement interpretation, compliance challenges, solution or application design, policies, procedures and any other subject related to the PCI PIN Security standard. The PCI PIN General Consulting provides assistance in analyzing Client's existing or planned PCI PIN 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 Point-to-Point Encryption (P2PE) solution, component or application.

Phase I: Onsite / Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on the PCI PIN environment.

SecureTrust will examine applicable design documentation to maximize the understanding of the PCI PIN environment's functionality, data handling processes, and design parameters, before delivering the PCI PIN General Consulting services.

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: General Consulting

The PCI PIN 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 PCI PIN security standard on which to focus the consulting services, as applicable.

SecureTrust will provide consulting around areas chosen by Client that relates to the PCI PIN environment, consulting will be delivered according to the PCI PIN security standard and requirements, discussing testing requirements and their applicability to the environment under review.

Example consulting activities may include:

- Interviews;
- Physical inspection of facilities and equipment;
- Identification of third parties used to support PCI PIN security operations, and a high-level assessment of the PCI DSS and PCI P2PE compliance of those third parties, if applicable; and
- Consulting on specific PCI PIN requirements.

SecureTrust will work with Client to identify and if possible, resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional information on the functions of the PCI PIN environment.

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

Phase III: Reporting

The PCI PIN 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 PCI PIN General Consulting activities.
- Provide Client with feedback on any findings identified during the service 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 PCI PIN version applicable at the time of the service start date.
 - The PCI PIN General Consulting does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
 - The PCI PIN General Consulting does not include visits to third parties used to support the PCI PIN environment, component or application.
 - The assessment consists of onsite or 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 services selected 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 create or modify Client documentation as part of PCI PIN General Consulting.
- SecureTrust will not provide remediation services as part of PCI PIN 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.