

Service Description

Payment Card Industry Card Production

General Consulting

Contents

- Payment Card Industry Card Production 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: Information Gathering..... 4
 - Phase II: General Consulting..... 5
 - Phase III: Reporting 5
 - SECURETRUST RESPONSIBILITIES 5
 - CLIENT RESPONSIBILITIES 6

Payment Card Industry Card Production General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Card Production (PCI CP) General Consulting (the "**Service**") is consulting by a Card Production Security Assessor (CPSA) for solution design, application design, policies, procedures and practices employed, or intended for use, by organizations to comply with the PCI CP logical and/or physical standards (the "**PCI CP standards**").

SecureTrust evaluates Client's policies, procedures and practices through documentation review, interviews, discussions, controls analysis, and examination of Client's current physical or logical security architectures.

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:

Card Production Security Assessor (CPSA) – A CPSA 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 CPSA 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 requirements of the PCI CP standards 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 CP standards or the review of a compensating control.

PCI CP General Consulting – A SecureTrust CPSA offers Client general consulting on requirement interpretation, compliance challenges, solution or application design, policies, procedures, and other subjects related to the PCI CP standards. SecureTrust assists Client in analyzing Client's existing or planned PCI CP security operations and safeguards through onsite 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.

The kickoff meeting also aims to verify the PCI CP functions to be the subject of consulting. The following PCI Card Production functions are defined by the PCI Security Standards Council (SSC):

- Card Production and Provisioning - Physical Security Requirements
- Card Production and Provisioning - Logical Security Requirements

Note that the Service may be for either, or both, PCI CP standards as determined during scoping.

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

Phase I: Information Gathering

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

SecureTrust will examine applicable documentation and may request a remote demonstration of Client's PCI CP environment function capabilities to maximize understanding of the card production and provisioning processes before delivering the Service.

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

- Security policies and procedures
- Key management
- Network security
- Roles and responsibilities, including personnel assignments
- Data security
- System security
- User management and access control
- Personal Identification Number (PIN) distribution
- Physical design parameters
- Collection of samples
- Packaging and delivery
- PIN printing

Phase II: General Consulting

The Service may take place onsite within Client's facilities. Some aspects of the PCI CP General Consulting may be delivered remotely, as determined by SecureTrust. A SecureTrust security consultant will work with Client to determine the areas of the PCI CP standards on which to focus the PCI CP General Consulting.

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

Example of consulting activities may include:

- Interviews
- Physical inspection of facilities and equipment
- Identification of use of third-party support for Client's PCI CP security operations, and a high-level assessment of the PCI CP compliance of those third parties, if applicable
- Consulting on specific PCI CP requirements
- Determination of critical assets
- Examination of business processes
- Identification of security and compliance management processes in place
- Review previous compliance or assessment documentation

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 CP standards and its responses. SecureTrust may request additional review of Client's PCI CP environment, documentation or processes and procedures.

The Service is not intended to focus on any specific controls, unless explicitly agreed to by SecureTrust and Client. The purpose of the Service is to assist Client in determining the best course of action for PCI CP focus areas and assist Client in making a determination of Client's ability to undergo a PCI CP compliance validation, and, where possible, to identify suggested priority areas for remediation. The Service is not a replacement for a PCI CP 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, 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 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 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 provide all necessary information requested by SecureTrust in the SecureTrust portal Compliance Manager assessment application according to agreed delivery dates per the high-level project plan.
- 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 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 version of PCI CP as applicable at the time of the Service start date.
 - The Service may consist of onsite and remote consulting activities.
 - 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 CP environment.
 - 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 CP 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 PCI CP General Consulting.
 - The validation of a third-party provider's PCI CP compliance is not included in 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.