SecureTrust
a Trustwave division

Service Description

Payment Card Industry Card Production

Pre-Assessment Workshop

Contents

Payment Card Industry Card Production Pre-Assessment Workshop

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Card Production (PCI CP) Pre-Assessment Workshop (the "**Service**") is high-level overview of compliance with the PCI CP logical or physical standards (the "**PCI CP standards**"), via an evaluation of the design and implementation of PCI CP controls and supporting policy, procedures and practices relevant to 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 Pre-Assessment Workshop – The PCI CP Pre-Assessment Workshop identifies high-level gaps and prioritizes areas that may require remediation to achieve compliance with the PCI CP standards.

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, deliverables, resource requirements and escalation procedures.

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 design documentation and may request a remote demonstration of Client's PCI CP environment to maximize understanding of the card production and provisioning processes before conducting the Service.

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

- 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: Pre-Assessment Workshop

SecureTrust will evaluate Client's PCI CP environment according to applicable PCI CP standards, and discuss testing requirements and their applicability to Client's PCI CP environment.

The Service may take place onsite within Client's facilities. Some aspects of the Service may be carried out remotely, as determined by SecureTrust. SecureTrust will work with Client to determine the high-level review requirements for each area of Client's PCI CP environment.

Example of the Service activities may include:

- Interviews
- Physical inspection of facilities and equipment
- Observation of performed processes and procedures in accordance with documentation collected during the Information Gathering phase

- High-level review of applicable PCI CP requirements
- High-level assessment of third-party relationships and provided third-party evidence of compliance with applicable requirements

SecureTrust will work with Client to resolve Client's assessment questions. SecureTrust will also provide the Client reasonable assistance in Client's interpretation of the PCI CP requirements 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. The goal of the Service is to make a determination of Client's ability to undergo a PCI CP validation, and to, where possible, identify suggested priority areas for remediation.

Phase III: Reporting

SecureTrust will develop a high-level executive summary report documenting observations and recommendations from the Service.

The draft report will be sent to Client and SecureTrust QA team for review. Client will be able to comment on and suggest changes to the report before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide an executive summary report as the final deliverable.

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, deliverables, and resource requirements.
- Schedule and conduct kickoff, periodic status, and closeout meetings.
- Interview appropriate organization personnel and collect information from personnel.
- Provide Client with information on any observations that require remediation.
- Produce an PCI CP high-level executive summary report.
- Deliver to Client a final PCI CP high-level executive summary report documenting observations and recommendations from the Service.

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, deliverables, 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 collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in the Service.
- 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 standards as applicable at the time of the Service start date.
    - The Service may consist of both onsite and remote assessment activities.
    - The Service does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - 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 Service.
    - 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.