SecureTrust
a Trustwave division

Service Description

Payment Card Industry Card Production

Gap Assessment

Contents

Payment Card Industry Card Production Gap Assessment 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: Review and Testing 4
Phase III: Reporting 5
SECURETRUST RESPONSIBILITIES 5
CLIENT RESPONSIBILITIES 6

Payment Card Industry Card Production Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Card Production (PCI CP) Gap Assessment (the "**Service**") is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the PCI CP logical or physical standards (the "**PCI CP standards**"). Specifically, SecureTrust evaluates Client's policies, procedures, and practices through documentation review, interviews, facilities inspections, 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 conducting the assessment, compliance determination and reporting.

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 Gap Assessment – SecureTrust identifies gaps and prioritizes areas that may require remediation to achieve compliance with the PCI CP standards. SecureTrust evaluates the necessary security

requirements to support the deployment and management of a card production environment. SecureTrust will provide a report detailing the results of the Service including areas of non-compliance.

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.

The kickoff meeting also aims to verify the applicable PCI CP functions to be assessed. 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

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 conduct interviews, as required, with architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and other Client personnel who may provide relevant details.

SecureTrust will examine applicable design documentation and may request a remote demonstration of Client's PCI CP environment to maximize understanding of Client's card production and provisioning processes before conducting the Review and Testing phase of 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: Review and Testing

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, controls analysis and examination of Client's current security architecture.

The review and testing may take place onsite within Client's facilities. Some aspects of testing may be carried out remotely, as determined by SecureTrust.

SecureTrust will examine Client's PCI CP environment according to PCI CP standards applicable as of the start date.

Where third parties are used to support Client's PCI CP environment, SecureTrust will collect information about the services provided and the relationships with such third parties.

SecureTrust and Client will work to determine the testing requirements for each area of Client's PCI CP environment. Testing activities may include:

- 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 CP environment

When sampling is permitted by the PCI CP testing procedures, SecureTrust will utilize non-statistical sampling, also known as judgement sampling, to determine the population and the sample.

Any areas of non-compliance identified will be communicated to Client's primary point of contact.

Compensating controls may be considered, at SecureTrust's sole discretion, when an entity cannot meet a PCI CP requirement explicitly as stated due to legitimate technical or documented business constraints provided that SecureTrust determines that the Client has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

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, applicable code areas, documentation, or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a PCI CP Gap Assessment Report documenting observations and recommendations from the Service. The PCI CP Gap Assessment Report may include details of non-compliance and may recommend specific changes to bring Client's PCI CP environment into compliance with the PCI CP standards.

The draft PCI CP Gap Assessment Report will be sent to Client for review. Client may comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final PCI CP Gap Assessment Report.

SecureTrust will provide a final PCI CP Gap Assessment Report.

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.
- Validate the scope of the Service.
- Create and respond to Client action items in Compliance Manager within SecureTrust portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform the Service against the applicable control testing procedures.
- Determine Service results and compliance status.
- Produce a draft PCI CP Gap Assessment Report.
- Deliver to Client a final PCI CP Gap Assessment 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 key steps, estimates for duration, environment information 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 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 the PCI CP standards as applicable at the time of the Service start date.
    - The Service may consist of both 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 CP services selected for a single SOW or Order Form must be for an identical term.
    - The Service start and end dates will be determined during the kickoff call.
    - 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.