SecureTrust
a Trustwave division

Service Description

Payment Card Industry Personal Identification Number (PCI PIN) Security Assessment

Contents

PCI PIN Security Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Personal Identification Number (PCI PIN) Security Assessment is (the "**Service**") is an assessment of security and procedural practices against the PCI PIN security requirements and the Qualified PIN Assessor (QPA) Program Guide as set out by the PCI Security Standards Council (the "Standard").

SecureTrust's PCI PIN Security Assessment and report on compliance (ROC) are delivered in accordance with the Standard and include specific brand guidance depending on the reporting requirements required by the payment brands.

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 conducting the assessment, compliance determination and reporting.

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 Security Assessment – The PCI PIN Security Assessment evaluates whether Client's PCI PIN environment is compliant with the Standard. SecureTrust will provide a report containing the results of the assessment including any areas of non-compliance. If areas of non-compliance are identified,

SecureTrust will prepare an action plan to assist in Client's remediation of non-compliant observations and overall compliance status.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate 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, 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 PIN environment.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's PCI PIN 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 have relevant details.

SecureTrust will examine applicable documentation and may request a remote demonstration of Client's system capabilities, including data handling processes and design parameters, before conducting the Security Controls Assessment phase.

Topics for Information Gathering may include, but are not limited to, the following:

- Policies and procedures
- Secure management of equipment used to process and manage PIN-related data;
- Third parties used to support Client's PCI PIN environment;
- Client's PCI PIN environment management processes;
- Point of Interaction (POI) device life cycle, including deployment, maintenance and decommissioning processes;
- Secure device management processes;
- PCI PIN environment processes; and
- Documented cryptographic operations and methodologies.

Phase II: Security Controls Assessment

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

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

SecureTrust will examine Client's PCI PIN environment according to applicable Standard testing requirements effective at the start date of the Service.

SecureTrust will work with Client to determine the appropriate testing requirements for each control objective of the Standard. Example testing activities may include:

- Examination of system configurations;
- Interviews;
- Observation of the practical implementation of policies, processes and procedures;
- Physical inspection of facilities and equipment;
- Observation of cryptographic operations and methodologies;
- Review of third parties used to support Client's PCI PIN environment.

In addition to Client's facilities, SecureTrust will need to perform on-site testing at any third-party key-injection facility (KIF), third-party POI device vendor/service provider, Certificate Authority/Registration Authority (CA/RA), storage facilities, etc.

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

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

Compensating controls may be considered, at SecureTrust's sole discretion when Client cannot meet a requirement explicitly as stated due to legitimate technical or documented business constraints if 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 the 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 processes and procedures.

For non-compliant observations, Client may remediate and provide relevant evidence that non-compliant observations have been remediated for up to the shorter of (i) 180 days following delivery of the final ROC or (ii) 45 days prior to the end of the Term of the Service as set out in the applicable SOW. Such parameters are based on estimated times to allow for reporting, quality assurance (QA), and the report submission processes.

Phase III: Reporting

SecureTrust will develop a report documenting observations and recommendations from the PCI PIN Security Assessment.

A draft report will be sent to Client for review. Client may comment and suggest changes to the draft report with supporting documentation. SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

SecureTrust will provide a final deliverable as defined below:

- If Client's PCI PIN environment is found compliant with the Standard, SecureTrust will provide Client with a compliant Report on Compliance (ROC) and complete an Attestation of Compliance (AOC) as a declaration of Client's compliance status.
- If Client' PCI PIN environment is found non-compliant with the Standard, SecureTrust will provide Client with a non-compliant ROC.

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.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Perform the PCI PIN Security Assessment against the applicable control testing procedures.
- Determine results and Client's compliance status.
- Identify to Client observations that may require remediation.
- Produce either a compliant or non-compliant ROC, depending on the status of Client's PCI PIN environment at the time the PCI PIN Security Assessment occurs.
- Deliver to Client a final report documenting observations and recommendations from the Service.
- Submit reporting documentation to card brands identified by Client.

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 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 may consist of both onsite and remote assessment activities.
    - The Service start and end dates will be determined during the kickoff call.
    - 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.
    - 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.

- For non-compliant observations, Client may remediate and provide relevant evidence that non-compliant observations have been remediated for up to the shorter of (i) 180 days following delivery of the final ROC or (ii) 45 days prior to the end of the Term of the Service as set out in the applicable SOW.
    - Should the remediation period start with less than 225 days before the end of the Service term stated in the applicable Order Form or SOW, then the remediation period will be shortened to end no later than 45 days prior to the Service term stated in the applicable Order Form or SOW.
- 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.