SecureTrust
a Trustwave division

Service Description

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

Contents

PCI PIN Security Assessment 3

Service Description 3
Base Service Features 3
SecureTrust Portal 3
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. 3
Global Compliance and Risk Services 3
Delivery and Implementation 4
Project Initiation 4
Phase I: Data Gathering 4
Phase II: Security Controls Assessment 4
Phase III: Reporting 5
SECURETRUST RESPONSIBILITIES 5
CLIENT RESPONSIBILITIES 6

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 a professional services engagement. The PCI PIN Security Assessment is an assessment of security and procedural practices against the PCI PIN requirements for organizations that process PIN data or perform key management activities in scope of the PCI Security Standards Council (PCI SSC) PCI PIN Program as required by participating payment brands. The PCI SSC's QPA Program leverages the requirements of the PCI PIN Security Requirements. SecureTrust is an approved Qualified PIN Assessor (QPA) company and is authorized to perform PCI PIN Security Assessments.

SecureTrust's PCI PIN Security Assessment and report on compliance are delivered in accordance with the PCI PIN Security Requirements and the QPA Program Guide, the assessment also includes specific brand guidance depending on the reporting requirements required by the payment brands.

BASE SERVICE FEATURES

SecureTrust's PCI PIN Security Assessment service 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 conducting the onsite assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and reporting quality assurance to the QPA and serves as a secondary point of contact for escalations and queries.

PCI PIN Security Assessment – An assessment to validate and report on Client's compliance status with the PCI PIN Security Requirements and QPA Program Guide. If areas of non-compliance are identified, SecureTrust will prepare an action plan to assist in remediation of non-compliant findings and overall compliance status. SecureTrust will provide a report containing the results of the assessment including any areas of non-compliance.

DELIVERY AND IMPLEMENTATION

The following is an overview of the assessment process. Depending on reporting requirements, Client should consult each brand's PIN program for additional guidance.

Project Initiation

The SecureTrust GCRS team is assigned to facilitate successful 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 the control environment.

Phase I: Data Gathering

SecureTrust will work with Client to gather and analyze information on the PIN environment. SecureTrust will conduct interviews, as required, with architects, developers, systems administrators, quality assurance (QA) and/or testing personnel, support staff, and other Client personnel who may provide relevant details on the PIN environment.

SecureTrust will examine applicable documentation and may request a remote demonstration of system capabilities to maximize understanding of the functions of PIN environment including data handling processes and design parameters, before conducting the PIN requirement review and portion of the assessment.

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

- Reviewing policies and procedures
- Secure management of equipment used to process and manage PIN-related data;
- Determination of third parties used to support the environment;
- Review of PIN environment management processes;
- Collection and review of applicable documentation;
- Point of Interaction (POI) device life cycle, including deployment, maintenance and decommissioning processes;
- Secure device management processes;
- PIN environment processes; and
- Review of documented cryptographic operations and methodologies.

Phase II: Security Controls Assessment

The PIN environment review will take place primarily within the Client's facilities. Some aspects of testing may be able to be carried out remotely. SecureTrust will work with Client to determine the testing requirements for each control objective of the PIN standard.

SecureTrust will examine the PIN environment according to all applicable PIN control objectives. Example testing activities may include:

- Observation of the practical implementation of policies, processes and procedures;
- Examination of system configurations;

- Interviews;
- Physical inspection of facilities and equipment;
- Observation of cryptographic operations and methodologies;
- Review of third parties used to support Client's PIN services (if applicable)

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.

Note: During the assessment, when sampling is permitted by the testing procedures, the QPA will utilize non-statistical sampling (often referred to as a judgement sampling) to determine the method of sampling, the number of items that will be examined, and which items to select.

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

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

For non-compliant findings, Client may remediate for up to 180 days following the Security Controls Assessment and provide relevant evidence that audit findings have been remediated. The Remediation Period ends no later than 45 days prior to the end of the applicable service term to allow for reporting, quality assurance (QA) and report submission processes.

Phase III: Reporting

SecureTrust will develop the report deliverable for submission to the SecureTrust Quality Assurance team for review. Once completed, the report will be sent to the Client.

SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

If there are no audit findings and SecureTrust has determined that Client is fully compliant, SecureTrust will provide the applicable cards brands with the PIN Report on Compliance (ROC) that includes detailed assessment findings, and the PIN Attestation on Compliance (AOC), which includes signatures of the QPA that conducted the assessment and an Executive Officer of Client.

SecureTrust will provide a final deliverable as defined below:

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

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, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.

- Validate scope of the engagement.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform controls assessment against the applicable control testing procedures.
- Provide Client with information on any findings that requires remediation.
- Determine assessment results and Client's status.
- Produce an assessment report.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.
- Submit reporting documentation to applicable card brands.

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, 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 compliance assessment 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 consists of both onsite and remote assessment activities.
    - The service period 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.
    - If there are non-compliance findings, the Remediation Period must start at least 225 days prior the end of the applicable service term.
        - Should the Remediation Period start with less than 225 days before the end of the applicable service term, then the Remediation Period will be shortened to end no later than 45 days prior to the applicable service term

- SecureTrust will not create or modify Client documentation as part of the PCI PIN Security Assessment.
- SecureTrust will not provide remediation services as part of the PCI PIN Security Assessment.
- 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.