SecureTrust
a Trustwave division

Service Description

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

Contents

PCI PIN Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Personal Identification Number (PCI PIN) Gap Assessment is a professional services engagement which assesses a Client's security and procedural practices against the requirements for organizations that process PIN data or perform key management activities related to PINs in accordance with the PCI Security Standards Council (SSC) Qualified Pin Assessor (QPA) Program. PCI SSC's QPA Program leverages the requirements of the PCI PIN version 3 Security Requirements. SecureTrust is a QPA Company and is authorized to perform PCI PIN Gap Assessments.

SecureTrust's PCI PIN Gap Assessment and gap assessment report are delivered in accordance with the PCI PIN Security Requirements and the QPA Program Guide.

The PCI PIN Gap Assessment involves an evaluation of various policies, procedures and practices through documentation review, interviews, facilities inspection and review of security architecture.

BASE SERVICE FEATURES

SecureTrust's PCI PIN Gap Assessment 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:

Security Consultant – 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 Security Consultant and serves Client as a secondary point of contact for escalations and queries.

PCI PIN Gap Assessment – An assessment to validate and report on Client's compliance status with the PCI PIN version 3 Security Requirements and the 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 areas of non-compliance, if any.

DELIVERY AND IMPLEMENTATION

The following is an overview of the assessment process.

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 the control environment.

Phase I: Discovery

SecureTrust will work with Client, where applicable, to:

- Determine critical assets;
- Examine business processes;
- Identify security and compliance management processes in place; and
- Review previous compliance or assessment documentation.

Phase II: Security Controls Assessment

SecureTrust will work with Client through interviews, discussions, and facilities inspections to:

- Gather and analyze pre-visit material for the gap assessment
- Examine applicable documentation
- Conduct demonstration of system capabilities

The goal of this phase of work is maximize understanding of Client's:

- PIN systems functionality
- Data handling processes
- Key management and design parameters prior to conducting onsite assessment

Topics to be covered in this phase of work include:

- Organization chart listing key management team members or participants
- Updated diagram flow of acquired PINs, PIN blocks and encryption keys from any point of entry through the point of exit
- Locations of facilities that perform cryptographic functions such as PIN translation, processing, verification and key storage, key creation, key injection/loading, as well as backup storage of cryptographic key materials
- Vendor product information for installed software that supports PIN environment and interchange processing
- Key inventory or key matrix
- Inventory of Encrypting PIN Pads (EPP) automated teller machines (ATMs), cash dispensers, kiosks, automated fuel dispensers (AFD), and point of sale (POS) terminals with PIN pads; including device type and locations, with the PCI PTS approval numbers (firmware version, application version, etc.)
- Inventory of secure cryptographic devices (SCD), including hardware (host) security module (HSM)
- List of operating parameters (such as allowing single-length keys) enabled at SCDs

- Purchase orders for applicable SCDs
- HSM command sets in use
- Total number of devices that are compliant with PCI PTS Device Security Requirements (Point of Interaction (POI) Modular Security Requirements)
- Key custodian agreements
- Documented procedures to support:
    - Key generation
    - Key storage
    - Key loading
    - Key distribution/conveyance
    - Key destruction
    - Key compromise
    - Compliance of cryptographic tools and devices
    - Device commissioning/decommission

Phase III: Security Controls Review / Testing

Testing will take place primarily within the Client's facilities, however some aspects of testing may be able to be carried out remotely. The SecureTrust QPA will work with Client to determine the testing requirements for each Control Objective of the PCI PIN Gap Assessment.

During this phase, the SecureTrust QPA will work with Client to resolve PCI PIN Gap Assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional demonstrations, reviews of documentation or reviews of processes and procedures.

Where third parties are used to support the PIN environment, SecureTrust will need to collect information about services provided by said third-parties, onsite assessment of third-party providers is not included in the gap assessment.

Example testing activities include:

- Reviewing policies and procedures
- Examination of system configurations
- Interviews
- Physical inspection of facilities and equipment
- Identification and high-level review of third parties used to support Client's PIN services (if applicable)

Note: During the PCI PIN Gap 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.

Phase IV: Reporting

SecureTrust will develop the PCI PIN Gap Assessment Report deliverable for submission to the SecureTrust Quality Assurance team for review. Once completed, the PCI PIN Gap Assessment Report will be sent to the Client.

SecureTrust retains final authority regarding the contents of the PCI PIN Gap Assessment Report and the type of final deliverable to be produced.

SecureTrust will securely manage and retain working papers and reports related to the PCI PIN Gap Assessment for six years, after which they will be securely destroyed.

SecureTrust will deliver the PCI PIN Gap Assessment Report all findings and recommendations from the assessment.

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 a gap assessment report.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

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 engagement consists of both onsite and remote assessment activities.
- The assessment 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.
- SecureTrust will not create or modify Client documentation as part of the PCI PIN Gap Assessment.
- SecureTrust will not provide remediation services as part of the PCI PIN Gap 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.