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 (PCI) Personal Identification Number (PIN) Gap Assessment (the "**Service**") assesses a Client's 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).

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 producing the report.

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 Standard or resolving complicated compliance questions and 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 Gap Assessment – The PCI PIN Gap Assessment identifies gaps and prioritizes areas that may require remediation to achieve compliance status with the Standard. SecureTrust will provide Client with the Service. SecureTrust will provide a report containing the results of the Service including areas of non-compliance. If areas of non-compliance are identified, SecureTrust will prepare an action plan to assist Client 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 design documentation and may request a remote demonstration of Client's system capabilities to maximize understanding of Client's PCI PIN environment, including data handling processes and design parameters, before conducting the Security Controls Assessment phase of the Service.

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

- Organization chart listing key management team members or participants
- Updated flow diagram 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, and 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

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 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 Security Controls Review and Testing phase may take place onsite within the Client's facilities. Some aspects of testing may be carried out remotely, as determined by SecureTrust.

Where third parties are used to support Client's PCI PIN environment, SecureTrust may need to collect information about such support. Onsite assessment of third-party providers is not included in the Service.

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

The SecureTrust QPA will work with Client to determine the testing requirements for each control objective of the Service. Example testing activities 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 virtually support Client's PCI PIN environment

Where sampling is permitted by the PCI PIN testing requirements, SecureTrust may utilize non-statistical (non-random) sampling, also known as judgement sampling, to determine the population and the sample.

SecureTrust may identify any areas of non-compliance identified to Client's primary point of contact.

SecureTrust may consider compensating controls, at SecureTrust's sole discretion, when Client cannot meet a PCI PIN requirement explicitly as stated due to legitimate technical or documented business constraints, provided that SecureTrust determines that 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 Standard and its responses. SecureTrust may request additional review of Client's PCI PIN environment, documentation or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a PCI PIN Gap Assessment Report documenting observations and recommendations from the PCI PIN Gap Assessment. The PCI PIN Gap Assessment Report may include

details of non-compliance and recommendations for specific changes that to bring Client's PCI PIN environment into compliance with the PCI PIN version 3 Security Requirements.

The draft PCI PIN Gap Assessment 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 final PCI PIN 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.
- 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.
- Identify to Client observations that may require remediation.
- Determine Service results and Client's compliance status.
- Produce a draft PCI PIN Gap Assessment Report.
- Deliver to Client a final PCI PIN 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 milestone dates, key steps, estimates for duration, deliverables, and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable Client's 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 may consist of both onsite and remote assessment activities.

- The Service start and end dates will be determined during a 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 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.