SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Pre-Assessment Workshop

Contents

P2PE Pre-Assessment Workshop

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point encryption (P2PE) Pre-Assessment Workshop (the "**Service**") is a high-level overview of compliance with the Payment Card Industry (PCI) Point-to-Point Encryption (P2PE) standard, via an evaluation of security requirements necessary to support the deployment of a secure P2PE solution, component or application, as required by the PCI P2PE standard and as set out by the PCI Security Standards Council (SSC) (the "**PCI P2PE standard**").

SecureTrust will evaluate policies, procedures and practices through documentation review, interviews, discussions, and examination of Client's current security architecture.

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:

P2PE Qualified Security Assessor (QSA) – A P2PE QSA is the primary resource for the fulfilment of the Service, responsible for conducting the workshop, compliance determination, and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the P2PE QSA as well as serves as a 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 P2PE standard 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 P2PE standard or the review of a compensating control.

P2PE Pre-Assessment – The Service identifies high-level gaps and prioritizes areas that may require immediate remediation to achieve compliance with the PCI P2PE standard. A SecureTrust P2PE QSA will

provide Client with a high-level analysis of Client's existing PCI P2PE security operations and safeguards through a series of workshops and consulting.

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.

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of Client's P2PE solution, component, or application.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's P2PE solution, component, or application.

SecureTrust will examine applicable design documentation to maximize the understanding of Client's P2PE solution, component, or application functionality, data handling processes, and design parameters, before conducting Phase II of the assessment.

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

- P2PE solution, component or application design;
- Determination of use of third-party support for Client's P2PE solution, component or application;
- Point of interaction (POI) device life cycle;
- Encryption/Decryption environment design; and
- Key life cycle.

Phase II: P2PE Pre-Assessment Workshop

The Service may take place onsite within the Client's facilities. Some aspects of the Service may be able to be carried out remotely. A SecureTrust P2PE QSA will work with Client to determine the high level review requirements for each domain of the P2PE standard, as applicable.

SecureTrust will evaluate the P2PE solution, component, or application according to applicable P2PE domains, discussing testing requirements and their applicability to the solution, component and/or application under review. Example pre-assessment workshop activities may include:

- Interviews;
- Physical inspection of facilities and equipment;
- Identification of use of third-party support for the solution, component or application, and a high-level assessment of the PCI DSS and PCI P2PE compliance of those third parties, if applicable; and
- High level review of applicable P2PE requirements.

SecureTrust will work with Client to identify and if possible, resolve Client's assessment questions and SecureTrust will provide Client reasonable assistance in Client's interpretation of the PCI P2PE standard

and its responses. SecureTrust may request additional review of Client's P2PE solution, component or application, documentation or data handling processes and procedures.

The Service is not intended to focus on any specific controls. The goal of the Service is to assess Client's ability to undergo a P2PE validation, and to, where possible, identify suggested priority areas for remediation.

Phase III: Reporting

SecureTrust will develop a high-level executive summary draft report that outlines areas of concern in relation to each P2PE domain, as applicable.

The draft report will be sent to Client for review. Client may comment on and suggest changes to the draft report before finalization. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide an executive summary final report as the final deliverable.

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, workshop and closeout meetings.
- Interview appropriate organization personnel and collect information from personnel.
- Conduct the Service.
- Identify to Client observations that require remediation.
- Produce executive summary report.
- Deliver to Client a final report documenting observations and recommendations from the Service.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- 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 collection of required 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.
    - SecureTrust uses the requirements and testing procedures of the current version applicable at the time of the Service start date.
    - The Service does not include in-depth testing or review of system settings, configurations, or observation of implemented processes and procedures.
    - The Service does not include visits to third parties used to support the P2PE solution, component, or application.
    - 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 services selected for a single SOW or Order Confirmation must be for an identical term.
    - The Service may consist of both onsite and remote assessment activities.
    - 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 retains final authority regarding the contents of the report and the type of final deliverable to be produced.
    - 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.