SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Designated Change Assessment

Contents

P2PE Designated Change Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point Encryption (P2PE) Designated Change Assessment (the "**Service**") is designed to assess changes made to a listed payment card industry (PCI) P2PE solution or component.

SecureTrust evaluates policies, procedures, and practices through documentation review, interviews, discussions, facilities inspections, controls analysis, 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 assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the P2PE QSA 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 requirements of the Payment Card Industry (PCI) P2PE standard as set out by the PCI Security Standards Council (SSC) (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 Designated Change Assessment – The Service includes an assessment of changes made to a listed P2PE solution or component. SecureTrust will provide Client with a report detailing the results of the Service.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates 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 an overview of the changes made to the Client's P2PE solution or component.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on changes made to Client's P2PE solution or component. SecureTrust will conduct interviews with solution architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and other Client personnel who may provide relevant details of Client's P2PE solution or component.

SecureTrust will examine applicable documentation and may request a remote demonstration of system capabilities to maximize understanding of the changes made to Client's P2PE solution or component functionality, data handling processes, and design parameters, before conducting the review and testing phase of the Service.

Phase II: Review and Testing

The review and testing will take place primarily onsite within the Client's facilities. Some aspects of testing may be carried out remotely. SecureTrust determine whether the testing requirements for each change have an impact on the changes made to the P2PE solution or component.

SecureTrust will examine changes to the P2PE solution or component according to applicable P2PE domain testing requirements.

Example testing activities include:

- Reviewing policies and procedures;
- Examination of system configurations;
- Interviews;
- Observation of the Client following documented processes, procedures and policies;
- Physical inspection of facilities and equipment;
- Performing payment transactions and forensic examinations; and
- Review use of third-party support for Client's P2PE solution or component, including (PCI DSS and PCI P2PE compliance of those third parties, if applicable.

SecureTrust will work with Client to 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 or component, documentation or processes and procedures.

Phase III: Reporting

SecureTrust will develop draft P2PE Designated Change report documenting observations and recommendations from Phase II.

The draft P2PE Designated Change report and any supporting documentation will be sent to Client for review. Client will be able to comment and suggest changes to the P2PE Designated Change report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide a final report deliverable, as defined below:

- If Client's P2PE solution or component is found to be compliant with the PCI P2PE standard, and once finalized by SecureTrust's QA group, the P2PE Designated Change documentation together with any required supporting documentation will be submitted to the PCI SSC for listing consideration.
- If Client's P2PE solution or component is found to be non-compliant with the PCI P2PE standard, SecureTrust will provide Client with non-compliant P2PE Designated Change documentation.

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.
- Validate the scope of the Service.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform the Service against the P2PE testing requirements enumerated at the start of the Service.
- Identify to Client any observations that require remediation.
- Determine Service results and solution or component compliance status.
- Produce either compliant or a non-compliant P2PE Designated Change Assessment documentation and submission documents, depending on the status of the solution or component at the time the validation occurs.
- 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 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.
    - SecureTrust's uses the P2PE Program Guide applicable to the version of the PCI P2PE standard for which the P2PE solution or component is currently validated.
    - 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.
    - The Service uses the requirements and testing procedures of the current PCI P2PE standard version applicable at the time of the Service start date.
    - The Service may consist of both remote and onsite assessment activities.
    - The Service will begin on the day of the kickoff call. The timeline and termination of the Service will be determined during the kickoff call.
    - Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the Service.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Service.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant observations, and one review of the Client remediated documentation.
    - All PCI Services selected for a single SOW or Order Form must be for an identical term.
    - Lab preparations are the responsibility of Client. Client must provide a lab for the testing that enables testing in accordance with the PCI P2PE standard. If testing is conducted in the SecureTrust Lab, Client must provide systems that are configured in accordance with the PCI P2PE standard.
    - 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.