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 is a professional services engagement. The P2PE Designated Change Assessment is designed to assess changes made to a listed P2PE solution or component.

The P2PE Designated Change Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection, controls assessment and examination of current security architecture.

BASE SERVICE FEATURES

SecureTrust's P2PE Designated Change 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:

P2PE Qualified Security Assessor (QSA) – An information security consultant and P2PE QSA 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 P2PE QSA as well as serves as a secondary point of contact for escalations and queries.

SecureTrust Compliance Review Board (CRB) – The CRB serves as an escalation point for requirement interpretation or complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is the final point of escalation for issue resolution regarding compliance status against requirement interpretation or the review of a compensating control.

P2PE Designated Change Assessment – An assessment of changes made to a listed P2PE Solution/Component. SecureTrust will provide Client with a P2PE Designated Change Assessment. SecureTrust will provide a report detailing the results of the P2PE Designated Change Assessment.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate the 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 an overview of the changes made to the P2PE solution/component.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on changes made to the 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 the 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 the P2PE solution or component functionality, data handling processes, and design parameters, before conducting the P2PE Designated Change Review and Testing portion of the assessment.

Phase II: Designated Change Review and Testing

The Designated Change Review and Testing 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 change as applicable to the P2PE domains and requirements impacted by the changes made to the P2PE solution or component.

SecureTrust will examine changes to the P2PE solution or component according to all applicable P2PE domain testing requirements. Example testing activities may 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 of third parties used to support the solution or component, including PCI DSS and PCI P2PE compliance of those third parties, if applicable.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional P2PE solution or component demonstrations, review of documentation or reviews of processes and procedures.

Phase III: Reporting

SecureTrust will develop P2PE Designated Change documentation for submission to the SecureTrust QA group for review.

The P2PE Designated Change documentation 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 documentation and supporting documentation before SecureTrust's QA group finalizes the report. SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

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

- If the P2PE solution or component is found to be compliant with the P2PE requirements, 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 the P2PE solution or component is found to be non-compliant with the P2PE requirements, SecureTrust will provide Client with non-compliant P2PE Designated Change documentation.

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 the scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform validation in accordance with the P2PE testing requirements as applicable to the designated change.
- Provide Client with information on any findings that requires remediation.
- Determine P2PE Designated Change results and solution/component compliance status.
- Produce either compliant or a non-compliant P2PE Designated Change documentation and submission documents, depending on the status of the solution or component at the time the validation occurs.
- 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.
    - 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.
    - SecureTrust's designated change assessment uses the requirements and testing procedures of the current P2PE version applicable at the time of the service start date.
    - The designated change assessment process consists of both remote and onsite assessment activities.
    - The designated change assessment process will begin on the day of the kickoff call. The timeline and termination of the designated change assessment process 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 designated change assessment process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the designated change assessment process.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant findings, and one review of the Client remediated documentation.
    - All services selected must be for an identical term.
    - The assessment consists of both onsite and remote assessment activities.
    - Lab preparations are the responsibility of Client. Client must provide a lab for the testing that enables testing in accordance with the P2PE requirements. If testing is conducted in the SecureTrust Lab, Client must provide systems that are configured in accordance with the P2PE requirements.
    - 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 P2PE Designated Change Assessment.
    - SecureTrust will not provide remediation services as part of the P2PE Designated Change 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.
- Pricing excludes the PCI SSC listing fee, payable per submission to the PCI SSC, the fee is levied directly by the PCI SSC.