SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Pre-Assessment Workshop

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

Contents

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

P2PE Pre-Assessment Workshop

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point encryption (P2PE) Pre-Assessment is a professional services engagement. The P2PE Pre-Assessment 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 P2PE standard.

Overview of the P2PE standard:

Domain 1: Encryption Device and Application Management	The secure management of the PCI-approved POI devices and the resident software.
Domain 2: Application Security	Not applicable to solution-only assessments.
Domain 3: P2PE Solution Management	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the P2PE Instruction Manual (PIM).
Domain 4: Merchant-managed Solutions	Separate duties and functions between merchant encryption and decryption environments.
Domain 5: Decryption Environment	The secure management of the environment that receives encrypted account data and decrypts it.
Domain 6: P2PE Cryptographic Key Operations and Device Management	Establish and administer key management operations for account data encryption POI devices and decryption HSMs.

The P2PE Pre-Assessment Workshop involves various policies, procedures and practices that will be evaluated by SecureTrust through interviews, documentation review and review of Client's current security architecture.

BASE SERVICE FEATURES

SecureTrust's P2PE Pre-Assessment Workshop includes the following standard features:

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

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 Pre-Assessment – An assessment to identify high-level gaps and prioritize areas that may require immediate remediation to achieve compliance with the PCI P2PE standard. The P2PE Pre-Assessment Workshop provides a high-level analysis of Client's existing PCI P2PE security operations and safeguards through a series of workshops and/or 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 the P2PE solution, component or application.

Phase I: Onsite / Remote Information Gathering

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

SecureTrust will examine applicable design documentation to maximize the understanding of the P2PE solution, component or application functionality, data handling processes, and design parameters, before conducting the P2PE Pre-Assessment Workshop portion of the assessment. Topics for information gathering may include, but are not limited to, the following:

- P2PE solution, component or application design;

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

- Determination of third parties used to support the solution;
- Point of interaction (POI) device life cycle;
- Encryption/Decryption environment design; and
- Key life cycle.

Phase II: Pre-Assessment Workshop

The P2PE Pre-Assessment will take place primarily within the Client's facilities. However, some aspects of the assessment may be able to be carried out remotely. A SecureTrust security consultant 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 all 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 third parties used to support 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 assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional information on the functions of the P2PE solution, component and/or application.

The pre-assessment workshop is not intended to focus on any specific controls. The goal of the pre-assessment workshop is to make a determination of Client's ability to undergo a P2PE validation, and to, where possible, identify areas of prioritization for remediation.

Phase III: Reporting

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

Once completed, the report will be sent to Client for review. Client will be able to comment on and suggest changes to the report before finalization. SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

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

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, workshop and closeout meetings.
- Interview appropriate organization personnel and collect information from personnel.

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

- Conduct the P2PE Pre-Assessment Workshop.
- Provide Client with information on any findings that requires remediation.
- Produce executive summary report.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the pre-assessment workshop.

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 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 workshop 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 PCI P2PE version applicable at the time of the service start date.
    - The P2PE Pre-Assessment Workshop does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - The P2PE Pre-Assessment Workshop 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 services selected must be for an identical term.
    - The assessment consists 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 will perform the service in the English language.
    - SecureTrust will not create or modify Client documentation as part of the P2PE Pre-Assessment Workshop.
    - SecureTrust will not provide remediation services as part of the P2PE Pre-Assessment Workshop.

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.

- 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.

Copyright © 2020 Trustwave Holdings, Inc. All rights reserved.