SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Gap Assessment

Contents

P2PE Gap Assessment 3
Service Description 3
Base Service Features 3
SecureTrust Portal 3
Global Compliance and Risk Services 4
Delivery and Implementation 4
Project Initiation 4
Phase I: Onsite and Remote Information Gathering 4
Phase II: Gap Assessment 5
Phase III: Reporting 5
SECURETRUST RESPONSIBILITIES 5
CLIENT RESPONSIBILITIES 6

P2PE Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point encryption (P2PE) Gap Assessment is a professional services engagement. The P2PE Gap Assessment helps to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the Payment Card Industry (PCI) P2PE standard. The P2PE Gap Assessment provides an analysis of PCI P2PE security operations and safeguards.

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	Secure applications in the P2PE environment.
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 Gap Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection and review of current security architecture.

BASE SERVICE FEATURES

SecureTrust's P2PE Gap 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 Gap Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the PCI P2PE standard. SecureTrust will provide Client with a P2PE Gap Assessment. SecureTrust will provide a report detailing the results of the P2PE Gap Assessment.

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 and Remote Information Gathering

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

SecureTrust will examine applicable design documentation to maximize understanding of the P2PE solution, component or application functionality, data handling processes, and design parameters, before conducting the P2PE Gap Assessment portion of the assessment.

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

- Collection of applicable vendor release agreements;
- Secure management of equipment used to encrypt account data;
- Determination of third parties used to support the solution;
- Review of solution management processes;

- Collection and review of applicable documentation;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Point of Interaction (POI) device life cycle, including deployment, maintenance and decommissioning processes;
- Secure device management processes;
- P2PE instruction manual review;
- Decryption environment processes; and
- Review of documented cryptographic operations and methodologies;

Phase II: Gap Assessment

The P2PE Gap Assessment will take place primarily within the Client's facilities. Some aspects of the assessment may be able to be carried out remotely. A SecureTrust security consultant will work with Client to determine the review requirements for each domain of the P2PE standard.

SecureTrust will examine the P2PE solution, component, application according to all applicable P2PE domain review requirements. Example testing activities may include:

- Observation of the practical implementation of policies, processes and procedures;
- Examination of system configurations;
- Interviews;
- Physical inspection of facilities and equipment; and
- Identification of third parties used to support the solution, component, application, and a high-level assessment of the 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 review of documentation or reviews of processes and procedures.

Phase III: Reporting

SecureTrust will develop a P2PE Gap Assessment Report document to identify any areas of non-compliance pertaining to the P2PE solution, component or application.

Included in the P2PE Gap Assessment Report are all non-compliant requirements, identified threats, vulnerabilities or potential vulnerabilities. This report includes recommendations to help eliminate or mitigate the risks to Client systems. Wherever possible, the report recommends specific changes that may be required to bring Client's P2PE solution, component or application into compliance with the P2PE standard.

The report will be sent to Client for review. Client will be able to comment 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 a P2PE Gap Assessment 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, 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 gap assessment against the P2PE testing procedures.
- Determine P2PE gap assessment results and solution, component or application compliance status.
- Produce a P2PE Gap assessment report on the status of the solution, component or application at the time the assessment 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 uses the requirements and testing procedures of the current PCI P2PE version applicable at the time of the service start date.
    - 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 P2PE Gap Assessment uses the requirements and testing procedures of the current P2PE version applicable at the time of the service start date.
    - The P2PE Gap Assessment process consists of both remote and onsite assessment activities.
    - The P2PE Gap Assessment process will begin on the day of the kickoff call. The timeline and termination of the P2PE Gap 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 P2PE gap assessment process.
    - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the P2PE gap 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.
- The P2PE Gap Assessment does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
- The P2PE Gap Assessment does not include visits to third parties used to support the P2PE solution, component or application.
- 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 Gap Assessment.
- SecureTrust will not provide remediation services as part of the P2PE Gap 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.