SecureTrust
a Trustwave division

Service Description

Non-listed Encryption Solution Assessment

Contents

Non-listed Encryption Solution Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Non-listed Encryption Solution Assessment (NESA) is a professional services engagement. The NESA is designed to identify gaps, and prioritize areas that may require remediation, to achieve adherence with the NESA guidance and to outline the gaps between the non-listed encryption solution and the Payment Card Industry (PCI) Point-to-Point Encryption (P2PE) standard. The NESA provides a gap analysis of a client's existing PCI P2PE security operations and safeguards.

SecureTrust's NESA uses the PCI P2PE Version Two requirements and testing procedures as the basis for the testing procedures, as well as the NESA guidance issued by the PCI Security Standards Council (SSC). The NESA guidance issued by the PCI SSC directs solution providers providing a non-listed encryption solution to conduct a gap analysis against the PCI P2PE with a minimum expectation that Domain five and Domain six of the PCI P2PE is met.

The NESA focuses on identifying compliance gaps in relation to process and procedures and as applicable for any third party key injection facility (KIF), point of interaction (POI) vendor/service provider, certificate authority (CA), storage facilities and/or decryption providers used to support the non-listed encryption solution in relation to the P2PE standard as detailed in the NESA guidance.

The NESA 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 NESA 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 and serves Client 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.

NESA – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve adherence with the NESA guidance and to outline the gaps between the non-listed encryption solution and the PCI P2PE standard. SecureTrust will provide Client with a NESA. SecureTrust will provide a report detailing the results of the NESA.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS teams are 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 non-listed encryption solution.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on the non-listed encryption solution. SecureTrust will conduct interviews with solution architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and others who may provide relevant details.

SecureTrust will examine applicable design documentation to maximize understanding of the non-listed encryption solution functionality, data handling processes, and design parameters before conducting the P2PE gap review portion of the NESA.

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

- Secure management of equipment used to encrypt account data;
- Determination of third parties used to support the solution;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Point of interaction (POI) device life cycle;
- Secure device management processes;
- Encryption and decryption environment management;
- Secure encryption methodologies;
- Cryptographic key generation methodologies;
- Cryptographic key distribution;
- Cryptographic key loading methodologies;
- Cryptographic key administration; and
- Secure application development processes.

Phase II: Non-listed Encryption Solution Assessment (NESA)

The NESA phase 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 as it relates to the non-listed encryption solution.

SecureTrust will examine the non-listed encryption solution according to each domain of the P2PE domains applicable to the non-listed encryption solution. Example testing activities include:

- Reviewing policies and procedures;
- Interviews;
- Physical inspection of facilities and equipment;
- Identification of third parties used to support the non-listed encryption solution, and a high-level assessment of the PCI DSS and P2PE compliance of those third parties, if applicable.

A SecureTrust security consultant 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, interviews or reviews of processes and procedures.

Phase III: Reporting

SecureTrust will develop a P2PE Report on Validation (P-RoV) outlining the current gaps in the non-listed encryption solution in relation to the P2PE standard as well as the NESA documentation as specified in the NESA guidelines issued by the PCI SSC. Included in the P-RoV are all compliant and non-compliant requirements. The NESA documentation will contain merchant-facing information, detailing the security functions of the non-listed encryption solution and the outcome of the NESA and the resultant findings.

The P-RoV will be sent to Client for review. Client will be able to comment and suggest changes to the P-RoV before SecureTrust finalizes the report. SecureTrust retains final authority with regard to the contents of the final report.

SecureTrust will provide a final deliverable, including the P-RoV and NESA 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 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.
- Provide Client with information on any findings that requires remediation.
- Determine current gaps in the non-listed encryption solution in relation to the P2PE standard and applicable P2PE testing procedures.
- Determine NESA results and Client compliance status.
- Produce the P2PE Gap P-RoV as detailed in the NESA guidance.

- Produce the NESA documentation as detailed in the NESA guidance.
- 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 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.
    - All services selected must be for an identical term.
    - The NESA does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
    - The NESA does not include visits to third-parties used to support the non-listed encryption solution.
    - The assessment consists of both onsite and remote assessment activities.
    - 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 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 NESA.
    - SecureTrust will not provide remediation services as part of the NESA.
    - SecureTrust will not provide a full PCI P2PE compliance validation.
    - 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.