SecureTrust
a Trustwave division

Service Description

Payment Card Industry

Token Service Provider Assessment

Contents

Payment Card Industry Token Service Provider Assessment 3

Service Description 3
Base Service Features 3
SecureTrust Portal 3
Global Compliance and Risk Services 3
Delivery and Implementation 4
Project Initiation 4
Phase I: Onsite and Remote Information Gathering 4
Phase II: Token Data Environment Review 4
Phase III: Reporting 5
SECURETRUST RESPONSIBILITIES 5
CLIENT RESPONSIBILITIES 5

Payment Card Industry Token Service Provider Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry (PCI) Token Service Provider (TSP) Assessment is a professional services engagement designed to validate whether identified security operations and controls have achieved the PCI TSP compliance objectives. The PCI TSP Assessment is an evaluation of the design and implementation of an organizations PCI TSP controls and supporting policy, procedures and relevant practices.

BASE SERVICE FEATURES

SecureTrust's PCI TSP 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:

Qualified Security Assessor (QSA) – An information security consultant and point to point encryption (P2PE) QSA is the primary resource for the fulfilment of the PCI TSP Assessment, 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 Security Consultant as well as 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.

PCI TSP Assessment – An assessment to validate whether Client's identified security operations and controls have achieved the PCI TSP compliance objectives. If Client is found compliant with the PCI TSP compliance objectives, SecureTrust will provide a TSP Report on Compliance (T-ROC) as a declaration of Client's compliance status. If Client is found non-compliant with the PCI TSP compliance objectives, SecureTrust will provide a non-compliant report detailing the results of the PCI TSP 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.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information about the token data environment (TDE). SecureTrust will conduct interviews, as required, with system architects, application developers, database developers, system administrators, quality assurance (QA) or testing personnel and other Client personnel who may provide relevant details on the TDE.

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

- Description of the TDE to provide a fundamental understanding;
- Description of the components that make up the TDE under review;
- Gather documentation of the TDE, including but not limited to diagrams and documentation illustrating the TDE internal/external data flows, including internal/external network communication, as applicable;
- List of hardware and software required to run the TDE, including any third-party dependencies, as applicable;
- Description of the TDE role in the payment lifecycle;
- Functional design specifications showing the TDE design and functional implementations;

In this phase, SecureTrust may request additional information to determine the testing needed to complete the PCI TSP review phase as outlined below.

Phase II: Token Data Environment Review

The TDE review focuses on logical testing of the TDE per the requirements outlined in the PCI TSP Assessment. The TDE review phase also includes any remaining interviews or documents reviews, as well as any processes that may require onsite observation. SecureTrust will obtain a thorough understanding of how the TDE processes data, how it is developed, distributed, configured and how it is protected from unauthorized access.

SecureTrust will examine the execution environment, including review of all tools, functions, software and hardware components, third-party and open source libraries, requirements and dependencies, as applicable.

SecureTrust will examine critical TDE parameters such as, but not limited to:

- Token generation, issuing, and mapping processes
- Assignment of token usage parameters
- Token lifecycle management
- Processes to map or re-map tokens, or perform de-tokenization
- Cryptographic processes to support tokenization functions
- Maintenance of underlying token security and related processing controls, such as domain restrictions during transaction processing.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and review Client responses. SecureTrust may request additional information, reviews of applicable areas, documentation, and/or data handling processes.

Phase III: Reporting

SecureTrust will develop report deliverables for submission to the SecureTrust Quality Assurance (QA) team for review.

Report deliverables will be sent to Client for review. Client may comment and suggest changes to the final deliverable and supporting documentation before SecureTrust's QA team 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 deliverable, as defined below:

- If the TDE is found compliant with the PCI TSP requirements, and once finalized by SecureTrust's QA team, the T-ROC will be submitted to the Client.
- If the TDE is found to be non-compliant with the PCI TSP requirements, SecureTrust will provide Client with a non-compliant report.

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 PCI TSP testing procedures.
- Provide Client with information on any findings that require remediation.
- Determine PCI TSP Assessment results and compliance status at the end of the PCI TSP Assessment process.
- Produce either a compliant or a non-compliant PCI T-ROC, depending on the compliance status at the time the PCI TSP Assessment occurs.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the PCI TSP 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 PCI TSP Assessment.
- 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 PCI TSP Assessment uses the requirements and testing procedures of the current PCI TSP version applicable at the time of the service start date.
    - The engagement consists of both remote and onsite assessment activities.
    - The PCI TSP Assessment process will begin on the day of the kickoff call. The timeline and end of the PCI TSP 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 PCI TSP Assessment process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the PCI TSP 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 PCI TSP Assessment includes one onsite assessment.
    - SecureTrust may request evidence from Client's systems and processes as required to assess 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 PCI TSP Assessment.
    - SecureTrust will not provide remediation services as part of the PCI TSP 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.