SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard

Self-Assessment Validation

Contents

PCI DSS Self-Assessment Validation

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Validation is a professional services engagement. The PCI DSS Self-Assessment Validation is designed to validate whether system components included in, or connected to, a cardholder data environment (CDE) are compliant with the PCI DSS.

BASE SERVICE FEATURES

SecureTrust's PCI DSS Self-Assessment Validation Service 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 QSA is the primary resource for the fulfilment of the service, responsible for performing the compliance assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight and reporting quality assurance to the QSA and serves as a secondary point of contact for escalations and queries.

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 and compensating control review.

PCI DSS Self-Assessment Validation – An assessment to validate and attest whether Client's identified system components included in, or connected to, the cardholder data environment (CDE) are compliant with the PCI DSS. If Client is found compliant with the PCI DSS, SecureTrust will provide a Self-Assessment Validation Report and countersign an Attestation of Compliance (AOC) as a declaration of Client's compliance status with the applicable client self-assessment questionnaire (SAQ). If Client is found non-compliant with the PCI DSS, SecureTrust will provide a non-compliant Self-Assessment Validation Report.

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: Discovery

Key Discovery activities include:

- Collect scoping documentation (discovery action items) via TrustKeeper prior to Phase II;
    - Scoping documentation may include, but is not limited to, policies and procedures, asset inventories, data flow diagrams, network diagrams, and other documentation which defines the environment.
- Agree on initial scope, including sampling methodology;
- Identification of initial action items or missing evidence; and
- Begin draft of a Self-Assessment Validation Report.

Phase II: PCI DSS Requirement Testing

Key PCI DSS Requirement Testing activities include:

- Perform interviews, discussions, facilities inspection & controls analysis;
- Collect test evidence via testing action items;
- If Client is eligible for sampling, and sample sets identify non-compliant items, SecureTrust will provide a self-assessment validation report with a non-compliant status as the final deliverable;
- Testing (remote and/or onsite):
    - Execution of test plans;
    - Evidence gathering; and
    - Evidence reviews.
- Identify remaining action items or missing evidence; and
- Continue drafting the Self-Assessment Validation Report.

Phase III: Final Deliverable

Key Final Deliverable activities include:

- Analyze evidence in accordance to the PCI DSS requirements; and
- Continue drafting the Self-Assessment Validation Report.

Phase IV: Quality Assurance

Key Quality Assurance activities include:

- Submission of report deliverable to SecureTrust Quality Assurance (QA) team for review; and
- Draft final Self-Assessment Validation Report.

Phase V: Closeout

Key Closeout activities include:

- Deliver final Self-Assessment Validation Report to Client point of contact and/or relevant reporting entities, summarizing the current state of Client's PCI DSS compliance;
- Countersign client AOC as a declaration of Client's compliance status if Client is found compliant with the PCI DSS; and
- 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, including segmentation, and discuss sampling methodology.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Determine compliance status for applicable controls in accordance with the PCI DSS.
- 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 assessment.
- Accurately respond to requests from SecureTrust when establishing contact and collecting information.
- Provide complete and accurate definition and documentation of in-scope systems.
- Make available Client resources capable of participating in assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Submit all evidence and complete remediation activities no later than five (5) days prior to the end of the assessment period.
- Client acknowledges:
    - SecureTrust will not complete an SAQ on behalf of Client. SecureTrust will provide a Self-Assessment Validation Report.
    - The service consists of remote and onsite assessment activities.
    - The service period start and end dates will be determined during the kickoff call.

- 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 PCI DSS Self-Assessment Validation service.
- SecureTrust will not provide remediation services as part of the PCI DSS Self-Assessment Validation service.
- 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.