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 (the "Service") designed to validate whether system components included in, or connected to, a cardholder data environment (CDE) are compliant with the PCI DSS as set out by the PCI Security Standards Council (the "Standard").

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between SecureTrust and Client.

BASE SERVICE FEATURES

The Service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal features consist of, among others, 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) – A QSA is the primary resource for the fulfilment of the Service, responsible for performing the validation, compliance determination and reporting.

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

Compliance Review Board (CRB) – The CRB serves as a final point for interpreting the requirements of the Standard or resolving complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is also the final point of escalation for issue resolution regarding compliance status against the requirements of the Standard or the review of a compensating control.

PCI DSS Self-Assessment Validation – to the PCI DSS Self-Assessment Validation validates whether Client's identified system components included in, or connected to, the cardholder data environment (CDE) are compliant with the Standard. If Client's in scope systems found compliant with the Standard, 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's in scope systems are found non-compliant with the Standard, SecureTrust will provide a non-compliant Self-Assessment Validation Report.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates 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: Information Gathering

SecureTrust and Client will work together to gather and analyze information about Client's in scope systems.

Key information gathering activities include:

- Collection of scoping documentation;
    - Scoping documentation may include, but is not limited to, policies and procedures, asset inventories, data flow diagrams, network diagrams, and other documentation which define Client's in scope systems.
- Agreement on initial in scope systems; and
- Identification of initial action items or missing evidence.

Phase II: PCI DSS Requirement Testing

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, controls analysis, and examination of Client's current security architecture.

SecureTrust will collect evidence via action items in the Compliance Manager application in the SecureTrust portal.

SecureTrust will determine if Client's in scope systems are eligible for sampling. If Client's in scope systems are eligible for sampling and sample sets identify non-compliant items, a second sample set will be collected. If the second sample set identifies non-compliant items, Client's in scope systems will be identified as non-compliant.

SecureTrust will analyze evidence in accordance with the Standard and determine the compliance status of Client's in scope systems.

Phase III: Final Deliverable

SecureTrust will develop a report documenting observations and recommendations from the Service.

The draft report will be sent to Client for review. Client may comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide Client with a final report deliverable, as defined below:

- If Client's in scope systems are found compliant with the Standard, and once finalized by SecureTrust's QA team, SecureTrust will provide Client with the Self-Assessment Validation Report and countersign Client's AOC as a declaration of Client's compliance status.

- If Client's in scope systems are found to be non-compliant with the Standard, SecureTrust will provide Client with a non-compliant Self-Assessment Validation report.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from 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 Service, including segmentation, and discuss sampling methodology.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Perform validation in accordance with the PCI DSS testing procedures.
- Provide Client with information on any observations that require remediation.
- Determine the compliance status of Client's in scope systems in accordance with the Standard.
- Produce either a compliant or a non-compliant final report, depending on the status of Client's in scope systems at the time the Service occurs.
- Deliver to Client a final report documenting all observations and recommendations from the assessment.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- Establish contact and remain available for communications from 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 definition and documentation of in-scope systems.
- Make available Client resources capable of participating in Service 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 may consist of remote and onsite assessment activities.
    - The project 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 Service.
- SecureTrust will not provide remediation services as part of the 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.