SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard Compliance Validation Service

Contents

PCI DSS COMPLIANCE VALIDATION SERVICE

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Compliance Validation Service (CVS) (the "**Service**") includes professional services to validate whether system components included in, or connected to, Client's cardholder data environment (CDE) are compliant with the PCI DSS as set out by the PCI Security Standards Council (the "Standard"). The Service also includes access to the SecureTrust Portal with applications to manage the engagement process and manage PCI external vulnerability scans.

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, the following key applications and functions:

Compliance Manager – The application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

PCI Manager – The application to manage unlimited PCI external vulnerability scans with an approved scanning vendor (ASV) certified scanner, and generate PCI ASV scan reports.

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 PCI DSS 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 PCI DSS or the review of a compensating control.

PCI DSS CVS – The Service validates whether Client's identified system components included in, or connected to, the CDE are compliant with the Standard. If Client's in scope systems are found compliant with the Standard, SecureTrust will provide a compliant Report on Compliance (ROC) and complete an

Attestation of Compliance (AOC) as a declaration of Client's compliance status. If Client's in scope systems are found non-compliant with the Standard, SecureTrust will provide a non-compliant ROC.

SecureTrust Quality Assurance (QA) – The SecureTrust QA team evaluates the ROC and controls findings before formal submission, as required by the PCI Security Standards Council. Once evaluation of the ROC is complete, SecureTrust's QA will finalize the ROC and AOC for delivery to Client and/or the relevant reporting entities.

Business-as-Usual (BAU) Review Meetings – BAU Review Meetings are used throughout the year to monitor and review the effectiveness of Client's security control processes in maintaining PCI DSS compliance on an ongoing basis. SecureTrust will provide Client with quarterly BAU Review Meetings.

Security Maturity Scores – Security Maturity Scores identify the maturity rating of Client's organization and help prioritize areas that may require remediation, to achieve compliance with the desired maturity level for Client's implementation of PCI DSS controls.

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 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.

SecureTrust will perform a PCI Readiness Check to determine Client's ability to complete the Service. If the PCI Readiness Check determines that Client is not ready to complete the Service or is not in compliance with the Standard, but an official statement on compliance is required, SecureTrust will provide Client with a non-compliant ROC.

Phase II: 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: Reporting

SecureTrust will develop a PCI DSS ROC 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, the ROC, together with required supporting documentation will be submitted to Client point of contact and/or relevant reporting entities.
- If Client's in scope systems are found to be non-compliant with the Standard, SecureTrust will provide Client with a non-compliant ROC.

SecureTrust will conduct a closeout meeting with Client.

BAU Review Meetings

SecureTrust will conduct BAU Review Meetings on a quarterly basis throughout the term of Service.

SecureTrust will complete and deliver a "BAU Review" spreadsheet to Client's point of contact for each BAU Review Meeting.

Security Maturity Scores

SecureTrust will conduct Security Maturity scoring as part of the Service.

SecureTrust will provide Client with Security Maturity scores for Client's implementation of PCI DSS controls and security control categories.

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 key steps, estimates for duration, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Perform the PCI readiness check.
- Validate scope of the Service, including segmentation, and discuss sampling methodology.
- Create and respond to Action Items in Compliance Manager within the SecureTrust Portal.

- Determine Client sampling eligibility.
- Perform validation in accordance with the Standard testing procedures.
- Identify to Client 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 PCI DSS ROC, depending on the status of Client's in scope systems at the time the Service occurs.
- Deliver to Client a final report documenting observations and recommendations from the Service.
- Conduct BAU Review Meetings.
- Conduct Security Maturity Scoring.

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 teams when establishing contact and collection of required information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in Service activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Agree to Service start and end dates.
- Submit all evidence and complete remediation activities no later than five (5) days prior to the end of the Service.
- Client acknowledges:
    - All security and feature updates for SecureTrust portal software will be included in major version release upgrades.
    - The Service may consist of both remote and onsite assessment activities.
    - The Service 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 for establishing 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 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.