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) is a subscription service. SecureTrust's PCI DSS CVS includes professional services to validate PCI DSS compliance and access to the SecureTrust Portal for vulnerability scanning and the Compliance Manager application.

BASE SERVICE FEATURES

SecureTrust's PCI DSS CVS includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among others, the following key applications and functions:

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

External Vulnerability Scanning (EVS) – Unlimited scans during the term producing reports with a high-level summary for executives and managers as well as detailed results and general remediation guidance for technicians. Remediation guidance includes Common Vulnerability and Exposures (CVE) linked vulnerability checks and best practices defined by SecureTrust.

Global Compliance and Risk Services

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Compliance Support Services (CSS) – Information security personnel monitor the progress of the assessment and initiate and follow-up on "action items" for Client, including submission of various types of evidence via Compliance Manager.

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.

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.

Compliance Assessment – An assessment to validate and attest whether Client's in scope systems are compliant with the PCI DSS. If Client is found compliant with the PCI DSS, 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 is found non-compliant with the PCI DSS, SecureTrust will provide a non-compliant ROC.

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

Business-as-Usual (BAU) Review – Meetings throughout the year to monitor and review the effectiveness of Client security control processes in maintaining PCI DSS compliance on an ongoing basis, as part of an entity's validation process.

Compliance Intelligence – An assessment to identify the maturity rating of Client's IT organization and help prioritize areas that may require remediation, to achieve compliance with the desired maturity level of an organization's implementation of PCI DSS controls and aid in implementing security best practice IT functions.

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

SecureTrust will collect information and documentation via the SecureTrust Portal and address initial action items or missing evidence.

SecureTrust will perform a PCI Readiness Check to determine ability to continue to Phase II. If the PCI Readiness Check determines that Client is not ready to complete the validation process or is not in compliance with the PCI DSS, but an official statement on compliance is required, SecureTrust will provide a non-compliant ROC.

SecureTrust will begin report deliverable development.

Phase II: PCI DSS Requirement Testing

SecureTrust will facilitate evidence gathering, interviews, discussions and perform evidence review, facilities inspection, testing (remote and onsite) and controls analysis. SecureTrust will collect test evidence via testing action items.

SecureTrust will determine if Client is eligible for sampling. If Client is 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 will be identified as non-compliant.

SecureTrust will continue development of the report deliverable.

Phase III: Final Deliverable

SecureTrust will analyze evidence in accordance with the PCI DSS, determine Client compliance status, and complete development of the report deliverable.

Phase IV: Quality Assurance

SecureTrust will submit the report deliverable to SecureTrust C-QA team for review and finalization.

SecureTrust C-QA team will evaluate the ROC, corroborate evidence, and review control findings and ratings to finalize the report deliverable.

Phase V: Closeout

SecureTrust will deliver the final report deliverable to Client point of contact and/or relevant reporting entities, summarizing the current state of Client's PCI DSS compliance.

SecureTrust will conduct a closeout meeting with Client.

BAU Review

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.

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 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 engagement, including segmentation, and discuss sampling methodology.
- Create and respond to Action Items in Compliance Manager within the SecureTrust Portal.
- Determine Client sampling eligibility.
- Determine Client compliance status in accordance with the PCI DSS.
- Provide a ROC.
- Conduct BAU review meetings.

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 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 compliance assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Agree to CVS assessment period start and end dates.
- Submit all evidence and complete remediation activities no later than five (5) days prior to the end of the CVS assessment period.
- Client acknowledges:
    - All security and feature updates for SecureTrust portal software will be included in major version release upgrades.
    - The service consists of both remote and onsite assessment activities.
    - The CVS assessment 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 Compliance Validation Service.
    - SecureTrust will not provide remediation services as part of the PCI DSS Compliance 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.