SecureTrust
a Trustwave division

Service Description

Secure Software Standard

Compliance Validation Service

Contents

Secure Software Standard Compliance Validation Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Secure Software Standard Compliance Validation Service (CVS) (the "**Service**") is designed to validate whether security functions, features and capabilities provided by payment software are compliant with the Payment Card Industry (PCI) Software Security Framework (SSF) Secure Software Standard. The Secure Software CVS is an evaluation of the design and implementation of security functions, features and capabilities provided by payment software and supporting policies, procedures, people, and practices relevant to the PCI SSF Secure Software 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:

SSF Assessor – An SSF Assessor is Client's primary resource during the Service and is responsible for conducting the assessment, evaluating compliance, and producing reports.

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

Compliance Review Board (CRB) – The CRB serves as a final escalation point for interpreting the requirements of the PCI SSF Secure Software 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 PCI SSF Secure Software standard or the review of a compensating control.

Secure Software CVS – SecureTrust evaluates whether Client's security functions, features, and capabilities provided by payment software are compliant with the PCI SSF Secure Software Standard. If

Client's payment software security functions, features, and capabilities are found compliant with the PCI SSF Secure Software Standard, SecureTrust will provide Client with a Report on Validation (ROV) as a declaration of Client's payment software's compliance status. If Client's payment software security functions, features, and capabilities are found non-compliant with the PCI SSF Secure Software Standard, SecureTrust will provide Client with a non-compliant ROV.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by 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.

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of Client's payment software.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information about Client's payment software. SecureTrust will conduct interviews, as required, with system architects, application developers, database developers, system administrators, quality assurance (QA), testing personnel, and other Client personnel who may have relevant details.

SecureTrust will examine applicable documentation and may request a remote demonstration of Client's payment software to understand the Client's payment software before conducting the Secure Software Validation phase.

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

- Client's payment software name, version number, supported operating systems, and any hardware or software requirements;
- Description of the components that make up Client's payment software;
- List of third-party dependencies related to Client's payment software and of development tools used during design, code development, and software integration, as applicable;
- Functional design and technical design documentation including description of Client's payment software data handling processes, design schema(s), data logging, and error handling behavior;
- Key management operations including any integrations with any third-party encryption functions, as applicable;
- Client's payment software interface diagrams and documentation illustrating Client's payment software interaction and data flow exchange with, but not limited to, third-party software, internal/external resources as well as any internal/external network communications, as applicable;
- List of software testing tools that may be required for lab testing, description of software test scripts and software test environment documentation for data processing, as applicable;
- Client implementation documentation including secure software integration procedures and recommendations for application integration into software deployment environments; and
- Details of testing and software evaluation lab location and requirements.

Phase II: Secure Software Validation

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

The Secure Software Validation phase will take place within SecureTrust's testing labs or at Client's premises, depending on logistical constraints and the nature of, and required systems for, Client's payment software as determined by SecureTrust.

SecureTrust will examine Client's payment software according to applicable PCI SSF Secure Software standard security requirements.

Where third parties are used to support Client's payment software, SecureTrust will collect information about the services provided by and the relationships with such third parties.

SecureTrust will work with Client to determine the testing requirements for each area of the PCI SSF Secure Software standard security requirements.

SecureTrust will review Client's payment software functionality, including end-to-end payment functionality, input and output functions, errors conditions, interfaces, data flows, cryptographic functionality, authentication mechanisms, and connections with other files/systems and components as applicable. SecureTrust will review the accuracy of Client's payment software documentation, including external customer facing documentation and internal documentation of Client's payment software functionality and implementation processes.

SecureTrust will examine Client's execution environment, including review of tools, functions, software API calls, software and hardware components, third-party and open source libraries, requirements, and dependencies, as applicable.

SecureTrust will perform static and dynamic analysis of Client's payment software, including using automated tools and manual testing techniques. This testing includes code review, software architecture review, penetration testing, application fuzzing, and vulnerability scanning, as applicable.

When sampling is permitted by the PCI SSF Secure Software standard testing procedures, SecureTrust will utilize non-statistical (non-random) sampling, also known as judgement sampling, to determine the population and the sample.

Compensating controls may be considered, at SecureTrust's sole discretion, when an entity cannot meet a PCI SSF Secure Software Standard explicitly as stated due to legitimate technical or documented business constraints if SecureTrust determines that the Client has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

SecureTrust will work with Client to resolve Client's assessment questions. SecureTrust will also provide the Client reasonable assistance in Client's interpretation of the PCI SSF Secure SLC standard and its responses. SecureTrust may request additional review of Client's SLC, documentation or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a draft 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 with supporting documentation. SecureTrust retains final authority regarding the contents of the final report and the type of deliverables to be produced.

SecureTrust will provide a final deliverable, as defined below:

- If Client's payment software is found compliant with the PCI SSF Secure Software Standard, the Report on Validation (ROV) and Attestation of Validation (AOV) together with required supporting documentation, will be submitted to the PCI Security Standards Council (SSC) for listing consideration.
- If Client's payment software is found to be non-compliant with the PCI SSF Secure Software Standard, SecureTrust will provide Client with a non-compliant ROV.

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 the agreed scope environment with regard to PCI SSF Secure Software Standard.
- Respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate Client personnel and collect information from personnel.
- Perform the Service in accordance with the Secure Software Standard testing procedures.
- Provide Client with information on observations that require remediation.
- Determine compliance results and software compliance status.
- Produce either a compliant or a non-compliant ROV, depending on the status of Client's payment software.
- Deliver to Client a final report documenting observations and recommendations from the assessment.

CLIENT RESPONSIBILITIES

- 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 details of the relevant environment and other business operations information.
- Make available resources capable of participating in the Service 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.
    - The Service uses the requirements and testing procedures of the current PCI SSF Secure Software Standard version applicable at the time of the Service start date.
    - The Service may consist of both remote and onsite assessment activities.
    - The Service will begin on the day of the kickoff call. The timeline and end of the Service 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 Service.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Service.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant observations, and one review of the Client remediated documentation.
    - The Service project includes one software evaluation and does include retesting of observations that require remediation.
    - Lab preparations are the responsibility of Client. Client must provide a lab for the application testing that complies with the PCI SSF Secure Software Standard requirements for the test environment. If testing is conducted in the SecureTrust lab, Client must provide systems that are configured in accordance with the PCI SSF Secure Software Standard.
    - When testing in the SecureTrust lab and where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has agreed to testing in the SecureTrust lab, and Client systems require special connectors or hardware, Client must supply the system components required to enable testing. SecureTrust will not provide operating system licenses or any other license required to test Client's software(s) in accordance with the PCI SSF Secure Software Standard requirements related to the software test environment.
    - 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 retains final authority regarding the contents of the report and the type of final deliverable to be produced.
    - 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.