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 (Secure Software CVS) is a professional services engagement. The Secure Software CVS is designed to validate if security functions, features and capabilities provided by payment software have achieved the Payment Card Industry (PCI) Secure Software Standard compliance objectives. 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 and the payment software under review.

BASE SERVICE FEATURES

SecureTrust's Secure Software CVS 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:

Security Consultant – An information security consultant and SSF Assessor who is the primary resource for the fulfilment of the service, responsible for conducting the assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and reporting quality assurance to the Security Consultant 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 or the review of a compensating control.

Secure Software CVS – An assessment to validate whether Client's security functions, features and capabilities provided by payment software have achieved the PCI SSF Secure Software Standard compliance objectives. If Client's security functions, features and capabilities provided by the payment software under review are found compliant with the PCI SSF Secure Software Standard requirements

and assessment procedure objectives, SecureTrust will provide a Report on Validation (ROV) as a declaration of the payment software's compliance status. If Client is found non-compliant with the PCI SSF Secure Software Standard compliance objectives, SecureTrust will provide a non-compliant report detailing the results of the Secure Software CVS.

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.

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

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information about the 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 provide relevant details on the software under review.

SecureTrust will examine applicable documentation and may request additional information and examples from Client in order for the Security Consultant to gain a clear picture of the software's design and capabilities.

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

- Description of the software to provide a fundamental understanding of the software to the assessor and for inclusion in the report deliverable;
- Software name and version number as well as supported operating systems and any hardware or software requirements;
- Description of the components that make up the software under review;
- List of any third-party dependencies required by the software as well as a list of development tools used during design, code development and software integration, as applicable;
- Functional design and technical design documentation including description of the software's 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;
- Software interface diagrams and documentation illustrating the software's 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

The Secure Software Validation will take place within SecureTrust's testing labs or at Client's premises, depending on the nature and required systems for the software under review, as well as depending on any logistical constraints. SecureTrust will work with Client to determine if an onsite visit is necessary or if testing can be done in the SecureTrust lab.

SecureTrust will review the software's 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 software documentation accuracy, including external customer documentation and accuracy of internal documentation to the software's functionality and implementation processes.

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

During the Software Evaluation, SecureTrust will perform static and dynamic analysis of the software, including using automated tools and manual testing techniques. This testing includes code review, software architecture review, penetration testing, application fuzzing and/or vulnerability scanning, as applicable.

The results of the software evaluation will provide a detailed report on the environment and any remediation steps that is required for the software to be deemed compliant with the Secure Software Standard requirements.

Phase III: Reporting

SecureTrust will develop a compliant Secure Software Standard ROV or a non-compliant report, depending on the status of the software at the time the validation occurs.

Report deliverables will be sent to Client for review. Client will be able to comment and suggest changes to the final deliverable and supporting documentation before SecureTrust's QA group finalizes the report.

SecureTrust will develop report deliverables for submission to the SecureTrust QA team for review.

SecureTrust will provide a final deliverable, as defined below:

- If the application is found compliant with the Secure Software Standard requirements, once finalized by SecureTrust's QA group, 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 the application is found to be non-compliant with the Secure Software Standard requirements, SecureTrust will provide Client with a non-compliant report.

SecureTrust will 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 the scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform validation in accordance with the Secure Software Standard testing procedures.
- Provide Client with information on any findings that requires remediation.
- Determine Secure Software Validation results and software compliance status at the end of the Secure Software Validation process.
- Produce either a compliant Secure Software Standard ROV or a non-compliant, depending on the status of the software at the time the validation occurs.
- 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 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 compliance assessment 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.
    - SecureTrust's Secure Software CVS uses the requirements and testing procedures of the current Secure Software Standard version applicable at the time of the service start date.
    - The engagement consists of both remote and onsite assessment activities.
    - The Secure Software Standard validation process will begin on the day of the kickoff call. The timeline and end of the Secure Software Standard validation process 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 Secure Software Standard validation process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Secure Software Standard validation process.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant findings, and one review of the Client remediated documentation.

- The Secure Software Standard validation process includes one software evaluation and does include retesting of findings that require remediation.
- Lab preparations are the responsibility of Client. Client must provide a lab for the application testing that complies with the 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 Secure Software Standard.
- When testing in the SecureTrust lab, where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has optioned for 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 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 Secure Software CVS.
- 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 Secure Software CVS.
- SecureTrust will not provide remediation services as part of the Secure Software CVS.
- 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.
- Pricing excludes the PCI SSC listing fee, payable per application deemed compliant and listed directly to the PCI SSC.