Service Description

Payment Application Data Security Standard

Application Security Review

Contents

Application Security Review

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Application Security Review is a professional services engagement. SecureTrust's Application Security Review is utilized to assess an application's overall security, and to determine whether the application qualifies for any of the eligibility criteria set forth in the Payment Application Data Security Standard (PA-DSS) Program Guide. The Application Security Review is an evaluation of the secure design and implementation of the application by assessing the application against the technical security controls outlined in the PA-DSS in an effort to determine the overall security posture of the application when deployed.

BASE SERVICE FEATURES

SecureTrust's Application Security Review includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application which manage the engagement process and collects and securely stores 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:

Payment Application Qualified Security Assessor (PA QSA) – An information security consultant and PA QSA is the primary resource for the fulfilment of the service, responsible for conducting the onsite assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and reporting quality assurance to the PA QSA and serves and 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.

Application Security Review – An assessment to validate whether Client's identified application security operations and controls operate in accordance with the technical controls outlined in the PA-DSS, the assessment also determines if the application qualifies for any of the eligibility criteria set forth in the PA-DSS Program Guide. If Client's application is found to be eligible for PA-DSS compliance validation, SecureTrust will provide Client with a proposal to undergo a full PA-DSS validation for listing with the Payment Card Industry Security Standards Council (PCI SSC). If Client's application is found to be ineligible for PA-DSS validation, SecureTrust will provide Client with a report that documents the application's existing security posture, which details why Client's application is not eligible for PA-DSS validation.

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: Information Gathering (Onsite / Remote)

SecureTrust will work with Client to gather and analyze information about the application. SecureTrust will conduct interviews with system architects, application developers, database developers, system administrators, quality assurance (QA) or testing personnel and other Client personnel who may provide relevant details on the application.

SecureTrust will examine applicable documentation and may request a remote demonstration of application capabilities.

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

- Description of the application to provide a fundamental understanding of the application to the assessor;
- Application name and version number as well as supported operating systems and any hardware requirements;
- Description of the components that make up the application under review;
- List of any third-party dependencies required by the application as well as a list of development tools used during design, code development and application integration, as applicable;
- Functional design and technical design documentation including description of application's data handling processes, design schema(s), data logging and error handling behavior;
- Data encryption implementation technique including integrations with any third-party encryption applications;
- Application interface diagrams and documentation illustrating application interaction and data flow exchange with third parties and merchant networks;
- Transaction flow diagram illustrating the application's data processing, inputs, and outputs to and from the application and to and from a merchant's network;
- 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; and
- Client implementation documentation including secure application integration procedures and recommendations for application integration into merchant environments.

Phase II: Application Review

The Application Review phase will take place within SecureTrust's testing labs or at Client's premises, depending on the nature and required systems for the application undergoing review and on logistical constraints. SecureTrust will work with Client to determine if an onsite visit is necessary or if testing can be done by SecureTrust remotely.

SecureTrust will gather a thorough understanding of how the application is configured and protected. SecureTrust may review business functions, administrative and organization capabilities, current functionality and requirements, as well as present and future initiatives. SecureTrust may examine critical application parameters such as database schema, logging, or error handling behaviors. SecureTrust may also review or verify written software development processes, relevant configuration data (e.g. network configuration documentation, production and test data), authentication features, change controls, data storage and encryption, audit logging, and remote maintenance features.

Functional testing of controls will be conducted as appropriate to determine the overall security posture of the application.

SecureTrust may request additional application details, review of applicable code areas, documentation, or data handling processes, as applicable to determine the PA-DSS eligibility of the application.

Phase III: Reporting & Deliverables

SecureTrust will develop a report deliverable documenting all findings and recommendations from the assessment.

SecureTrust will provide a report deliverable, as defined below:

- If Client’s application is found to be eligible for PA-DSS compliance validation, SecureTrust will provide Client with a proposal to undergo a full PA-DSS validation for listing with the PCI SSC.
- If Client’s application is found not to be eligible for PA-DSS compliance validation, SecureTrust will provide Client a report that documents the application’s existing security posture, allowing SecureTrust to detail why Client’s application is not eligible for PA-DSS validation.

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 within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform evaluation of the application against the PA-DSS eligibility criteria.
- Determine application PA-DSS eligibility status.
- Produce either a proposal to undergo full PA-DSS validation, or a report that documents the application’s existing security posture detailing why the application is not eligible for PA-DSS validation, depending on the status of the application at the time the assessment 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 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.
- Client acknowledges:
  - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
  - SecureTrust's Application Security Review uses the eligibility criteria of the current PA-DSS version applicable at the time of the service start date.
  - The Application Security Review consists of both remote and onsite assessment activities.
  - The assessment period will begin on the first day of the onsite component of the engagement. The timeline and end dates will be determined during the kickoff call. Client must submit all evidence and provide requested information no later than business forty-five (45) days prior to the end of the assessment period.
  - 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 inaccurate information provided by Client.
  - SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the assessment.
  - SecureTrust will perform the service in the English language.
  - SecureTrust will not create or modify Client documentation as part of the Application Security Review.
  - SecureTrust will not provide remediation services as part of the Application Security Review.
  - SecureTrust will not offer any legal guidance or counseling.
  - The quality and accuracy of the Application Security Review is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.