SecureTrust
a Trustwave division

Service Description

Payment Application Data Security Standard

Low-Impact Change Assessment

Contents

PA-DSS – Low-Impact Change Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Application Data Security Standard (PA-DSS) Low-Impact Change Assessment is a professional services engagement. SecureTrust's PA-DSS Low-Impact Change Assessment is designed to validate whether identified payment application security operations and controls have achieved the PA-DSS compliance objectives. The PA-DSS Low-Impact Change Assessment is an evaluation of application version changes and supporting policy, procedures and practices relevant to the PA-DSS.

BASE SERVICE FEATURES

SecureTrust's PA-DSS Low-Impact Change Assessment 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:

Qualified Security Assessor (QSA) – An information security consultant and Payment Application QSA (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 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.

PA-DSS Low-Impact Change Assessment – For application version changes that qualify as a Low-Impact Change, SecureTrust will perform application testing, as described in the PA-DSS program guide, on the changes specified by the vendor for the new version with the goal of generating a "Delta" report on validation (ROV) and Change analysis documentation. If Client is found compliant with the PA-DSS compliance objectives, SecureTrust will provide a Report on Validation (RoV) as a declaration of Client's compliance status. If Client is found non-compliant with the PA-DSS compliance objectives, SecureTrust will provide a non-compliant report detailing the results of the PA-DSS Low-Impact Change Assessment.

The ROV and change analysis documents will be submitted to the PCI Security Standards Council (SSC) for listing consideration

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: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information about the application. SecureTrust will conduct interviews, as required, 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.

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

- Description of the application to provide a fundamental understanding of the application;
- Application name and version number as well as supported operating systems and any hardware or software requirements;
- Description of the components that make up the application under review;
- List of hardware and software required to run the application, including any third-party dependencies, as applicable;
- Description of the application's role in the payment lifecycle, including authorization and settlement functions, as applicable;
- Software Development Lifecycle (SDLC) processes;
- Functional design specifications showing the application design and functional implementations;
- Key management operations including any integrations with any third-party encryption functions, as applicable;
- Application interface diagrams and documentation illustrating the application's internal/external data flows, including internal/external network communication, as applicable;
- List of application testing tools that may be required for lab testing;
- Description of payment application test scripts and application test environment documentation for data processing, as applicable;
- Client implementation documentation including secure application integration procedures and recommendations for application integration into merchant environments.

In this phase, SecureTrust may request a remote demonstration of the application to determine the testing needed to complete the PA-DSS CVS application review phase as outlined below.

Phase II: Application Review

The application review will take place within SecureTrust's testing labs or at Client's premises, depending on the nature of, and required systems for, the application 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.

The application review focuses on logical testing of the application per the requirements outlined in the PA-DSS. The application review phase also includes any remaining interviews or documents reviews, as well as any processes that may require onsite observation. SecureTrust will obtain a thorough understanding of how the application processes data, how it is developed, distributed, configured and how it is protected from unauthorized access.

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

SecureTrust will examine critical application parameters such as, but not limited to, data handling processes, database schemas, logging and error conditions. SecureTrust may also verify written software development processes, review relevant application configurations, production and test data, authentication features, change controls, data storage and encryption, audit logging, and remote maintenance features. SecureTrust will conduct functional testing of controls as appropriate to determine the application's compliance with the PA-DSS controls.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and review Client responses. SecureTrust may request additional application demonstrations, reviews of applicable code areas, documentation, and/or data handling processes.

As part of the application review phase, SecureTrust will perform a penetration test either remotely or within the testing labs. The test will determine how secure the application is from common vulnerabilities and from vulnerabilities as listed by the PA-DSS, as applicable. SecureTrust will provide Client with a report detailing the results of the penetration test including any remediation steps that are required for the application to meet PA-DSS controls. For web based applications, an in-depth test must be performed to determine the compliant status of the application and that test is not included as part of the application review.

Phase III: Reporting

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

Report deliverables will be sent to Client for review. Client may comment and suggest changes to the final deliverable and supporting documentation before SecureTrust's QA group finalizes the report. SecureTrust retains final authority regarding the contents of the report and the type of final deliverable to be produced.

SecureTrust will provide a final deliverable, as defined below:

- If the application is found compliant with the PA-DSS requirements, and once finalized by SecureTrust's QA group, the redlined RoV, together with required supporting documentation will be submitted to the PCI SSC for listing consideration.
- If the application is found to be non-compliant with the PA-DSS 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 within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform validation in accordance with the PA-DSS testing procedures.
- Provide Client with information on any findings that requires remediation.
- Determine PA-DSS validation results and application compliance status at the end of the PA-DSS validation process.
- Produce either a compliant or a non-compliant PA-DSS RoV, depending on the status of the application 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 teams 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 PA-DSS Low-Impact Change Assessment uses the requirements and testing procedures of the current PA-DSS version applicable at the time of the service start date.
    - The engagement consists of both remote and onsite assessment activities.
    - The PA-DSS validation process will begin on the day of the kickoff call. The timeline and end of the PA-DSS 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 PA-DSS validation process.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the PA-DSS 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 PA-DSS Low-Impact Change Assessment includes one application assessment.
- The PA-DSS Low-Impact Change Assessment does not include web based application penetrations tests.
- Lab preparations are the responsibility of Client. Client must provide a lab for the application testing that complies with the PCI Data Security Standard (PCI DSS) controls in accordance with Appendix B of the PA-DSS. If testing is conducted in the SecureTrust PA-DSS lab, Client must provide systems that are configured in accordance with the PA-DSS and the PCI DSS.
- When testing in the SecureTrust PA-DSS Lab, where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has optioned for testing in the SecureTrust PA-DSS lab and Client systems require special licenses, 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 application(s) in accordance with the PA-DSS requirements related to the application test environment.
- SecureTrust may request evidence from Client's systems and processes as required to assess compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
- Pricing excludes the PCI SSC listing fee, payable per application deemed compliant and listed directly to the PCI SSC.
- 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 PA-DSS Low-Impact Change Assessment.
- SecureTrust will not provide remediation services as part of the PA-DSS Low-Impact Change Assessment.
- 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.