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 (the "**Service**") is designed to validate whether identified payment application security operations and controls have achieved compliance with the PA-DSS as set forth by the Payment Card Industry Security Standards Council (PCI SSC) (the "**PA-DSS**"). The Service is an evaluation of application version changes and supporting policy, procedures and practices relevant to the PA-DSS.

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:

Payment Application Qualified Security Assessor (QSA) – A PA QSA 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 report quality assurance to the PA QSA as well as serves as Client's secondary point of contact for escalations and queries.

Compliance Review Board (CRB) – The CRB serves as a final point for interpreting the requirements of the PA-DSS 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 PA-DSS 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's application is found compliant with the PA-DSS, SecureTrust will provide a Report on Validation (ROV) as a declaration of Client's compliance

status. If Client's application is found non-compliant with the PA-DSS, SecureTrust will provide a non-compliant ROV detailing the results of the Service.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates 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

SecureTrust and Client will work to gather and analyze information about Client's 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 Client's application.

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

- Description of Client's application to provide a fundamental understanding of Client's 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 Client's application;
- List of hardware and software required to run Client's application, including any third-party dependencies, as applicable;
- Description of Client's application's role in the payment lifecycle, including authorization and settlement functions, as applicable;
- Software Development Lifecycle (SDLC) processes;
- Functional design specifications showing Client's 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 Client's 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.

SecureTrust may request a remote demonstration of Client's application to determine the testing needed to complete the application review phase as outlined below.

Phase II: Application Review

The application review 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 application.

SecureTrust will work with Client to determine if an onsite visit is necessary or if testing can be done within the SecureTrust's testing labs.

The application review phase focuses on logical testing of Client's 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 onsite process observations. SecureTrust will obtain a thorough understanding of how Client's application processes data, how it is developed, distributed, configured and how it is protected from unauthorized access.

SecureTrust will examine Client's 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 Client's critical application parameters such as, but not limited to, data handling processes, database schemas, logging and error conditions. SecureTrust may also verify Client's 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 Client's application's compliance with the PA-DSS.

SecureTrust will work with Client to resolve Client's assessment questions and SecureTrust will provide Client reasonable assistance in Client's interpretation of the PA-DSS and its responses. SecureTrust may request additional review of Client's application, applicable code areas, documentation or data handling processes and procedures.

SecureTrust will perform an application penetration test either remotely or within SecureTrust's testing labs. The test will determine how secure Client's 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 application penetration test including any remediation steps that are required for Client's application to achieve compliance with the PA-DSS. For web-based applications, an in-depth test must be performed to determine the compliance status of Client's application and that test is not included as part of the Service.

Phase III: Reporting

SecureTrust will develop a 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 and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide a final deliverable, as defined below:

- If Client's application is found compliant with the PA-DSS, and once finalized by SecureTrust's QA team, the redlined ROV, together with required supporting documentation will be submitted to the PCI SSC for listing consideration.
- If Client's application is found to be non-compliant with the PA-DSS requirements, 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 scope of the Service.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform the Service in accordance with the PA-DSS testing procedures.
- Identify to Client any observations that require remediation.
- Determine Service results and application compliance status at the end of the Service.
- Produce either a compliant or a non-compliant PA-DSS ROV, depending on the status of the application at the time the Service occurs.
- Deliver to Client a final report documenting all observations and recommendations from the Service.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- 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 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.
    - The Service uses the requirements and testing procedures of the current PA-DSS 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 includes one application assessment.
- The Service 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 lab, Client must provide systems that are configured in accordance with the PA-DSS and the PCI DSS.
- When testing in the SecureTrust lab, 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 licenses, connectors or hardware, Client must supply the system components required to enable testing and bear any related cost. SecureTrust will not procure 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. Client will provide a seat, license, special testing role authorization, or other form of authorized access to SecureTrust if required for SecureTrust to use any of Client's relevant applications.
- SecureTrust may request evidence from Client's systems and processes as required to assess compliance with any specific requirements. Client will 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 for establishing 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 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.