SecureTrust
a Trustwave division

Service Description

Payment Application Data Security Standard

No-Impact Change Assessment

Contents

PA-DSS – No-Impact Change Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Application Data Security Standard (PA-DSS) No-Impact Change Assessment (the "**Service**") is designed to determine whether changes outlined in the Vendor Change Analysis document qualify as a no-impact change. The Service is an evaluation of the Vendor Change Analysis document 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 No-Impact Change Assessment – SecureTrust will collect a Vendor Change Analysis document from Client that outlines the changes made to Client's application. If SecureTrust can determine that the change qualifies as a no-impact change, SecureTrust will produce the necessary change documentation and submit to the PCI Security Standards Council (SSC) for review and acceptance for inclusion as an update to the current listing of the application.

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:

- Detailed information on the changes being made to Client's application;
- Updated implementation guide;
- Application name and version number.

In this phase, 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 remotely and does not include any application testing, the application review phase consist purely of analysis of the changes being made to Client's application to determine that they truly have no impact on Client's application security or on PA-DSS controls.

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 group 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 the change to Client's application is found to be a no-impact change, and once finalized by SecureTrust's QA group, the necessary change documentation will be submitted to the PCI SSC for listing consideration.
- If the change to Client's application is not found to be a no-impact change, SecureTrust will provide Client with a response to the Vendor Change Analysis document.

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 the final deliverables, including the PA QSA Change Impact document and attestation of validation (AOV)
- Submit final change documentation to the PCI SSC, if applicable.

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 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 PA-DSS version applicable at the time of the Service start date.
    - The Service consists of remote 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 onsite testing or testing in the SecureTrust lab.
- 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 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.