

Service Description

Payment Application Data Security Standard

No-Impact Change Assessment

Contents

PA-DSS – No-Impact Change Assessment	3
Service Description	3
Base Service Features	3
SecureTrust Portal.....	3
Global Compliance and Risk Services	3
Delivery and Implementation.....	4
Project Initiation	4
Phase I: Onsite and Remote Information Gathering	4
Phase II: Application Review	4
Phase III: Reporting.....	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES.....	5

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 is a professional services engagement. SecureTrust's PA-DSS No-Impact Change Assessment is designed to determine whether changes outlined in the Vendor Change Analysis document qualify as a no-impact change. The PA-DSS No-Impact Change Assessment is an evaluation of the Vendor Change Analysis document and supporting policy, procedures and practices relevant to the PA-DSS.

BASE SERVICE FEATURES

SecureTrust's PA-DSS No-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 fulfillment 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 No-Impact Change Assessment – SecureTrust will collect a Vendor Change Analysis document from Client that outlines the changes made to the application. If SecureTrust can determine that the change qualifies as a no-impact change, SecureTrust will produce the necessary change documentation and submit the no-impact change 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 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:

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

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

The No-Impact Change Assessment does not include an onsite visit or testing in the SecureTrust lab.

Phase III: Reporting

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

Once finalized by SecureTrust QA, the 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 change 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 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 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 the final deliverables, including the PA-QSA Change Impact document and AoV
- If found compliant, submit final reporting documentation to the PCI SSC.

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 No-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 remote 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 No-Impact Change Assessment includes one application assessment.
- The PA-DSS No-Impact Change Assessment 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 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 No-Impact Change Assessment.
- SecureTrust will not provide remediation services as part of the PA-DSS No-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.