Service Description

Payment Card Industry Three Domain Secure (PCI 3DS)
Core Security Assessment
Contents

PCI 3DS Core Security 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: PCI 3DS Review and Testing ...............................................................................................5
  Phase III: Reporting .............................................................................................................................5
  Phase IV: Client Debrief .......................................................................................................................5
SECURETRUST RESPONSIBILITIES .................................................................................................5
CLIENT RESPONSIBILITIES ..............................................................................................................6
PCI 3DS Core Security Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust’s Payment Card Industry Three Domain Secure (PCI 3DS) Core Security Assessment is a professional services engagement. The PCI 3DS Core Security Assessment is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the PCI 3DS standard. The PCI 3DS Core Security Assessment provides an analysis of existing PCI 3DS security operations and safeguards.

Overview of the PCI 3DS standard:

| Part 1: Baseline Security Requirements | A baseline of technical and operational security requirements designed to protect the PCI 3DS data environment (3DE) |
| Part 2: PCI 3DS Security Requirements | Security requirements to protect PCI 3DS data and processes |

The PCI 3DS Core Security Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, application testing, controls assessment and examination of current security architecture including code review of the application code base.

BASE SERVICE FEATURES

SecureTrust’s PCI 3DS Core Security 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 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 Client 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.

PCI 3DS Core Security Assessment – An assessment to identify gaps and prioritize areas that may require remediation to achieve compliance with the PCI 3DS standard. SecureTrust will provide Client with a PCI 3DS Core Security Assessment through evaluation of security requirements necessary to support the deployment and management of a PCI 3DS function. SecureTrust will provide a report detailing the results of the PCI 3DS Core Security Assessment.

**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.

The kickoff meeting also aims to verify the PCI 3DS function being assessed. The following PCI 3DS functions are defined by the PCI SSC:

- 3DS Server (3DSS)
- 3DS Directory Server (DS)
- 3DS Access Control Server (ACS)

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of the PCI 3DS data environment.

**Phase I: Onsite and Remote Information Gathering**

SecureTrust will work with Client to gather and analyze information on the PCI 3DS data environment. SecureTrust will conduct interviews, as required, with system architects, developers, systems administrators, QA or testing personnel, support staff, and other members of the PCI 3DS data environment function teams.

SecureTrust will examine applicable documentation and may request a remote demonstration of the PCI 3DS data environment function capabilities to maximize understanding of the data handling processes and design parameters before conducting the PCI 3DS Review and Testing portion of the assessment.

Topics covered during this phase of work include:

- Policies and procedures
- Key management
- Configuration standards
- Vulnerability management
- Access control
- Media management
- Incident response
- System development life cycle (SDLC)
• Security governance
• Data management
• Risk management

Phase II: PCI 3DS Review and Testing
The PCI 3DS Review and Testing will take place primarily within the Client’s facilities. Some aspects of testing may be carried out remotely. The SecureTrust security consultant will work with Client to determine the testing requirements for each area of the PCI 3DS functions being assessed.

A SecureTrust security consultant will work with Client to resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional PCI 3DS data environment demonstrations, reviews of applicable areas, documentation, or data handling processes, as needed.

During the review and testing phase, SecureTrust will examine the PCI 3DS data environment according to all applicable PCI 3DS requirements. Example testing activities include:

• Examination of system configurations
• Interviews
• Observation of performed processes and procedures in accordance with documentation collected during Phase I
• Physical inspection of facilities and equipment
• Review of third-party relationships and provided third-party evidence of compliance with applicable controls

The above list may change based on the scope of the PCI 3DS Core Security Assessment.

Phase III: Reporting
SecureTrust will develop a report deliverable for submission to the SecureTrust Quality Assurance (QA) team for review.

Phase IV: Client Debrief
Report deliverables will be sent to Client for review. Client will be able to comment and suggest changes to the report and supporting documentation before SecureTrust’s QA team 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, including the report and associated documentation, as defined below:

• If the PCI 3DS data environment is found compliant with the PCI 3DS requirements, and once finalized by SecureTrust’s QA team, SecureTrust will provide a compliant report with required supporting documentation to Client.
• If the PCI 3DS data environment is found non-compliant with the PCI 3DS 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 against the PCI 3DS testing requirements.
• Provide Client with information on any findings that requires remediation.
• Determine PCI 3DS evaluation results and compliance status.
• Produce either a compliant or a non-compliant report, depending on the status of the PCI 3DS data environment 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:
  o All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
  o SecureTrust’s PCI 3DS Core Security Assessment uses the requirements and testing procedures of the current version applicable at the time of the service start date.
  o SecureTrust may collect evidence from applicable test systems, including system files, application files, database contents and images of test systems, as needed.
  o Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the assessment process.
    ▪ Client must submit all evidence and complete remediation activities no later than forty five (45) days prior to the end of the assessment process.
  o 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.
- Lab preparations are the responsibility of Client. Client must provide the systems required for lab testing to ensure all applicable requirements can be tested, even if testing is conducted at the SecureTrust premises.
- When testing in the SecureTrust lab, where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has optioned for testing in the SecureTrust lab, and Client systems require special 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 PCI 3DS requirements related to the test environment.
- 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.
- All services selected must be for an identical term.
- The assessment consists of both onsite and remote assessment activities.
- 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 PCI 3DS Core Security Assessment.
- SecureTrust will perform the service in the English language.
- The review and determination of a third party provider’s PCI 3DS compliance is not included in the PCI 3DS Core Security Assessment.
- SecureTrust will not create or modify Client documentation as part of the PCI 3DS Core Security Assessment.
- SecureTrust will not provide remediation services as part of the PCI 3DS Core Security Assessment.
- SecureTrust will not offer any legal guidance or counseling.
- The quality and accuracy of the PCI 3DS Core Security Assessment is dependent on Client’s provision of accurate information and access to Client systems and resources to SecureTrust.