SecureTrust
a Trustwave division

Service Description

Payment Card Industry Three Domain Secure (PCI 3DS) Gap Assessment

Contents

PCI 3DS Gap 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: Information Gathering 4
Phase II: Review and Testing 4
Phase III: Reporting 5
SECURETRUST RESPONSIBILITIES 5
CLIENT RESPONSIBILITIES 6

PCI 3DS Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Three Domain Secure (PCI 3DS) Gap Assessment (the "**Service**") is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the PCI 3DS standards set out by the PCI Security Standards Council (SSC) (the "**PCI 3DS standard**").

SecureTrust evaluates policies, procedures, and practices through documentation review, interviews, discussions, evidence reviews, facilities inspections, application testing, controls analysis, and examination of Client's current security architecture including code review of Client's application code base.

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:

Qualified Security Assessor (QSA) – A 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 QSA and 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 PCI 3DS standard 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 PCI 3DS standard or the review of a compensating control.

PCI 3DS Gap Assessment – The PCI 3DS Gap Assessment identifies gaps and prioritizes areas that may require remediation to achieve compliance with the PCI 3DS standard. SecureTrust evaluates security requirements necessary to support the deployment and management of Client's PCI 3DS function. SecureTrust will provide a report detailing the results of the PCI 3DS Gap Assessment.

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.

The kickoff meeting also aims to verify Client's PCI 3DS function. 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 Client's PCI 3DS data environment.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on the PCI 3DS data environment. SecureTrust will conduct interviews, as required, with system architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and other Client personnel who may provide relevant details.

SecureTrust will examine applicable documentation and may request from Client a remote demonstration of the PCI 3DS data environment capabilities to maximize understanding of the data handling processes and design parameters before conducting the review and testing phase of the Service.

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

- 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: Review and Testing

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, application testing, controls analysis and examination of Client's current security architecture including code review of Client's application code base.

The review and testing phase may take place onsite within the Client's facilities. Some aspects of testing may be carried out remotely, as determined by SecureTrust.

SecureTrust will examine Client's PCI 3DS data environment according to applicable PCI 3DS testing requirements applicable at the Service start date.

The SecureTrust QSA will work with Client to determine the testing requirements for each area of Client's PCI 3DS functions. Example testing activities include:

- Review of policies and procedures
- Examination of system configurations
- Interviews
- Observation of performed processes and procedures in accordance with documentation collected during the information gathering phase
- Physical inspection of facilities and equipment
- Identification and high level review of third parties used to support Client's PCI 3DS data environment

When sampling is permitted by the testing procedures, SecureTrust may utilize non-statistical sampling, also known as judgement sampling, to determine the population and the sample.

SecureTrust will communicate any identified areas of non-compliance with the PCI 3DS standard to Client's primary point of contact.

Compensating controls may be considered, at SecureTrust's sole discretion, when an entity cannot meet a PCI 3DS requirement explicitly as stated due to legitimate technical or documented business constraints provided that SecureTrust determines that the Client has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

SecureTrust will work with Client to resolve Client's assessment questions. SecureTrust will also provide Client reasonable assistance in Client's interpretation of the PCI 3DS standard and its responses. SecureTrust may request additional review of Client's PCI 3DS data environment, documentation, or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a report documenting observations and recommendations from the Service. A 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, including the report and associated documentation, as defined below:

- If Client's PCI 3DS data environment is found compliant with the PCI 3DS standard, and once finalized by SecureTrust's QA team, SecureTrust will provide Client with a compliant ROC and complete an Attestation of Compliance (AOC) as a declaration of Client's compliance status.
- If Client's PCI 3DS data environment is found non-compliant with the PCI 3DS standard, SecureTrust will provide Client with a non-compliant ROC.

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.
- Interview appropriate organization personnel and collect information from personnel.
- Validate the scope of the Service.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Perform the Service against the PCI 3DS testing requirements enumerated at the start date of the Service.
- Determine the Service results and compliance status.
- Identify to Client any observations that require remediation.
- Produce either a compliant or a non-compliant ROC, depending on the status of Client's PCI 3DS data environment at the time the Service occurs.
- Deliver to Client a final report documenting observations and recommendations from the Service.

CLIENT RESPONSIBILITIES

- 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 the 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 version applicable at the time of the Service start date.
    - SecureTrust may collect evidence from applicable test systems, including system files, application files, database contents and images of test systems, as needed.
    - 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.

- 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 agreed to testing in the SecureTrust lab, and Client systems require special 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 PCI 3DS requirements related to the 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 prove compliance with any specific requirements. Client will provide all such evidence in a timely manner.
- All PCI services selected for a single SOW or Order Form must be for an identical term.
- The Service may consist 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 Service.
- 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 Service.
- 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.