

Service Description

Payment Card Industry Data Security Standard
Compliance Readiness Subject Matter Expert Consulting

Contents

PCI DSS Compliance Readiness Subject Matter Expert Consulting	3
Service Description	3
Base Service Features	3
SecureTrust Portal.....	3
Global Compliance & Risk Services	3
Delivery and implementation.....	4
Project Initiation	4
PCI DSS Compliance Readiness SME Consulting	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS	4

PCI DSS Compliance Readiness Subject Matter Expert Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Compliance Readiness Subject Matter Expert (SME) Consulting (the "Service") is designed to assist and guide organizations in preparing for, achieving and maintaining compliance with the PCI DSS as set out by the PCI Security Standards Council (the "Standard").

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 & 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 fulfillment of the Service and is responsible for scheduling and conducting consulting activities.

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 requirements of the 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 Standard or the review of a compensating control.

PCI DSS Compliance Readiness SME Consulting – Consulting assistance and guidance for primary documentation, scoping and other activities in preparation of a PCI DSS compliance assessment. SecureTrust will provide Client with consulting to assist and guide Client in completion of tasks required to successfully articulate and demonstrate the implementation of controls to achieve compliance with the Standard.

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.

PCI DSS Compliance Readiness SME Consulting

SecureTrust will provide the Service with regard to primary documentation, scoping, and other activities in preparation of a PCI DSS compliance assessment. SecureTrust will assist Client in creation and/or modification of documentation, diagrams and evidence required to achieve and maintain PCI DSS compliance. Service activities may include, but are not limited to, the following topics:

- Critical concepts for achieving and demonstrating PCI DSS compliance;
- Expectations of Client seeking to achieve PCI DSS compliance from the QSA;
- Preparation and guidance for individuals who will come in contact with the QSA;
- Testing procedures;
- Evidence requirements;
- Periodic requirements in the Standard;
- Required administrative, technical and physical security controls for PCI DSS compliance; and
- Scope of the cardholder data environment (CDE), including:
 - Asset inventory, asset types, and scoping rationale;
 - Network diagram and data flow diagram illustrating systems, network connections to the CDE and assets from the asset inventory; and
 - Segmentation of CDE and planned sampling methodology.

SecureTrust will conduct a closeout meeting with Client, if desired.

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 and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.

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 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 engagement consists of remote consulting activities.
 - SecureTrust will perform the Service in the English language.
 - 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 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.