

Service Description

Information Security Risk Assessment Remediation

Contents

Information Security Risk Assessment Remediation	3
Service Description	3
Base Service features	3
SecureTrust Portal.....	3
Global Compliance & Risk Services	3
Delivery and implementation.....	4
Project Initiation	4
Remote Consulting Engagement.....	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES.....	4

Information Security Risk Assessment Remediation

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Information Security Risk Assessment (ISRA) Remediation (the "**Service**") is designed to assist and guide Client in remediation of risks identified as the result of an information security risk assessment.

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:

Security Consultant – A Security Consultant is Client's primary resource during 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 Security Consultant and serves as Client's secondary point of contact for escalations and queries.

ISRA Remediation – SecureTrust provides remote consulting on the remediation of risks identified as the result of an information security risk assessment. SecureTrust will work with Client to develop prioritized action plans and processes for remediation of such risks.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by scheduling and conducting a 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.

Remote Consulting Engagement

The Security Consultant will work with Client and provide guidance and recommendations to create prioritized action plans and targeted processes for remediation. The Service activities may include guidance or recommendations on one or more of the following areas:

- Business processes or applications that transmit, process, or store critical data;
- Network infrastructure;
- Security infrastructure;
- Security procedures or guidelines;
- Information security policy; and
- Governance charter.

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

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 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 consists of remote consulting activities.
 - SecureTrust may request information about Client's systems and processes as required to describe Client data privacy management programs. Client agrees to provide all such information in a timely manner.
 - 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 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.