SecureTrust
a Trustwave division

Service Description

Onsite Chief Information Security Officer

Contents

Onsite Chief Information Security Officer

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Onsite Chief Information Security Officer (Onsite-CISO) Service (the "**Service**") helps Client develop and maintain information security, risk management, and compliance management programs.

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:

Security Consultant – A senior, management-level, 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.

Onsite-CISO Service – Consulting by one or more senior, management-level, Security Consultants with a strong balance of business acumen, technology expertise, and experience in information security, risk management, and compliance management programs. The Security Consultant will assist and guide Client in the development of its information security, risk management, and compliance management programs.

DELIVERY AND IMPLEMENTATION

Project Initiation

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

Security Consultant and Client Collaboration

The Security Consultant will interview and collaborate with Client's management team to understand Client's business objectives, stakeholders, general business policies, and acceptable risk levels as driven by business priorities. The Security Consultant will interview and work with Client to identify critical IT assets and operations, including data, systems, applications, infrastructure, and relevant policy and procedures.

The Security Consultant will work with Client to examine business processes and to identify information protection requirements, security practices, and compliance management processes already in place. Based on this information, the Security Consultant will help Client identify threats, vulnerabilities, and the potential likelihood and impact of risk events applicable to Client's line of business and to Client's specific operations. The Security Consultant will guide Client on way to optimize its efforts and resource allocations.

The Service may also include (at SecureTrust's discretion):

- Knowledge transfer from the Security Consultant to Client representatives to enable security related decisions which support Client's business objectives.
- Objective, experienced, security recommendations based on an understanding of Client's environment and SecureTrust solutions, independent of Client's internal biases and politics.
- Review of Client's security posture, including risk assessment and decision support for ongoing operations, changes, and new Client initiatives.
- Jargon-free communications and presentations of security status directed at all levels of management, IT, and operational staff.
- Support Client's request for proposal (RFP) development and response activities as well as vendor risk management activities.
- Support Client's business continuity and incident response planning activities.

SecureTrust's Security Consultant will work with Client as needed and will be available for regularly scheduled meetings and activity with reasonable advance notification once a mutual agreement is reached regarding scheduling and logistics.

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.
- Respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Be available for regularly scheduled meetings and activity.

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 may consist of onsite and remote consulting activities.
    - The Service start and end dates will be determined during the kickoff call.
    - 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.
    - 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 may create or modify Client documentation as appropriate for the industry accepted role of a chief information security officer.
    - SecureTrust may perform remediation services as appropriate for the industry accepted role of a chief information security officer.
    - SecureTrust will provide remediation guidance and assist in prioritization of remediation efforts to achieve Client's objectives.
    - SecureTrust will not offer any legal guidance or counseling. The Service does not guarantee compliance with data privacy regulatory requirements or other regulatory requirements. Client is responsible for making all management decisions with regard to its data privacy policies.
    - 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.