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 is a professional services engagement. The Onsite-CISO service helps to develop and maintain information risk, security and compliance management programs.

BASE SERVICE FEATURES

SecureTrust's Onsite-CISO 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:

Information Security Consultant – A senior, management-level information security consultant and QSA is the primary resource for the fulfilment of the service.

Managing Consultant (MC) – An MC provides guidance, project oversight and reporting quality assurance to the Security Consultant and serves Client as a secondary point of contact for escalations and queries.

Onsite-CISO Service – Consulting by one or more senior, management-level consultants with a strong balance of business acumen and technology knowledge, as well as considerable depth in information risk, security, and compliance management. SecureTrust will assist and guide Client in development of information risk, security, and compliance management programs.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the service which includes 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.

SecureTrust will assess Client's readiness to begin the engagement by confirming that appropriate information is documented and required resources are available.

Phase I: Client Collaboration

SecureTrust's Onsite-CISO will interview and collaborate with Client's management team, to gain an understanding of the business objectives, stakeholders, general business policies, and gain an understanding of acceptable risk levels driven by business priorities. The Onsite-CISO will interview and work with Client to identify critical IT assets and operations, including data, systems, applications, infrastructure, and relevant policy and procedures.

SecureTrust's Onsite-CISO will work with Client to determine critical assets, examine business processes, and identify information protection requirements as well as security and compliance management processes in place. Once this information is understood, the Onsite-CISO will help Client identify threats and potential impacts which are applicable to Client's line and business, and specific to Client's operations. The Onsite-CISO will provide Client vision and guidance to optimize its efforts and resource allocations to ensure recommended policies, procedures, and technologies support business priorities.

Additionally, SecureTrust's Onsite-CISO may provide:

- Knowledge transfer, 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, and independent of Client's internal assumptions and political mechanisms
- Continuous review of Client's security posture, providing risk assessment and decision support in support of ongoing operations, changes, and new Client initiatives
- Jargon-free communications and presentations of security status to all levels of management, IT, and operational staff
- Represent Client organization to third parties in support of RFP development and response as well as vendor risk management
- Business continuity and incident response planning

SecureTrust's Onsite-CISO 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 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 scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Work with Client as needed and be available for regularly scheduled meetings and activity.

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 consulting 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 onsite consulting activities.
    - The assessment period 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 assessment.
    - 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's Onsite-CISO 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 objectives.
    - SecureTrust will not offer any legal guidance or counseling. The provision of an Onsite-CISO does not guarantee compliance with data privacy regulation. 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.