SecureTrust
a Trustwave division

Service Description

Data Privacy Gap Assessment

Contents

Data Privacy Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Gap Assessment (the "Service") is designed to identify gaps to help achieve compliance with the privacy regulatory requirements specified in the applicable Order Form or SOW ("Privacy Requirements").

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 Security Consultant is the primary resource for the fulfilment of the Service, gap determination, and reporting.

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.

Data Privacy Gap Assessment – An assessment to identify gaps in Client's organization based on the Privacy Requirements and offer recommendations. SecureTrust will provide a final report that identifies gaps that Client must remediate to achieve compliance with the Privacy Requirements.

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.

Phase I: Information Gathering

SecureTrust will interview appropriate personnel, including third parties as required, to understand the details of Client's people, processes, and technology that support compliance with Privacy Requirements.

SecureTrust's consultants will collect information relevant to Client's compliance with Privacy Requirements.

Each interview requires a peer-level group of participants from a corporate level and features a series of brainstorming activities. The format of all interviews is the same for each process, but the audience differs to include senior management, operational area management and other business and information technology personnel.

Key activities include:

- Schedule a site visit or remote workshop to identify required documentation.
- Understand business goals and strategic directions that impact the handling of personally identifiable information with regard to compliance with privacy regulation.
- Review business operations including internally-performed and outsourced processes.
- Review key organizational documentation, including Client's policies and procedures.

Phase II: Data Privacy Gap Assessment

SecureTrust and Client will work, through interviews, discussions, and documentation review, to identify critical people, processes, and technology that support compliance with Privacy Requirements. This process will identify gaps that Client must remediate to achieve compliance with the Privacy Requirements.

Key activities include:

- Remote meetings and onsite visits to conduct interviews and discussions.
- Review people, process and technology that support compliance with privacy regulation.
- Reconciliation of existing policies and procedures to support compliance with privacy regulation.
- Document the Service results.

Phase III: Reporting

SecureTrust will develop a report document to identify any areas of non-compliance. The report includes details of non-compliant observations and recommends specific changes that may be required to bring Client's environment into compliance with the Privacy Requirements.

A draft of the report will be sent to Client and SecureTrust Quality Assurance (QA) for review. Client will be able to comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. The SecureTrust QA team will review and suggest changes to finalize the draft report. SecureTrust retains final authority regarding the contents of the final report.

SecureTrust will provide a final report.

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.
- Validate scope of the Service.
- Create and respond to Client Action Items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine Service results.
- Provide Client with information on any observations that require remediation.
- Produce a draft report.
- Deliver to Client a final report documenting observations and recommendations from the Service.

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 environment information and configuration requirements.
- Inform SecureTrust of 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.
- Submit all evidence in accordance with the milestone dates.
- Client acknowledges:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - Personnel from the following departments are generally involved:
        - Operations, Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
        - Third party data brokers, controllers or processors are involved.
    - The Service may consist of both remote and onsite activities.
    - The Service project start and end dates will be determined during the kickoff call.
    - SecureTrust may request evidence from Client's processes as required to demonstrate compliance with privacy regulation. 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 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 provision of the Service does not guarantee compliance with Privacy 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.