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 is a professional services engagement. The Data Privacy Gap Assessment is designed to identify gaps to achieving compliance with privacy regulation.

BASE SERVICE FEATURES

SecureTrust's Data Privacy Gap Assessment includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application to manage the engagement process and 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 – An information security consultant is the primary resource for the fulfilment of the service, responsible for performing the assessment, gap determination and reporting.

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

Data Privacy Gap Assessment – An assessment to identify gaps to achieve compliance with the privacy regulatory requirements and offer recommendations. SecureTrust will provide a Data Privacy Gap Assessment Report as a declaration of Client's gaps to achieving compliance with the privacy regulation.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate 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.

Project initiation activities include:

- Introduction to the SecureTrust Compliance Manager application for managing the assessment and/or data sharing.

Outputs of Project Initiation activity include:

- Agreement on the high-level project plan
- Regular project status meetings with key stakeholders

Phase I: Discovery

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

SecureTrust's consultants will collect information relevant to compliance with privacy regulation.

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.

Outputs include:

- Schedule of site visits, remote workshops and interviews.

Phase II: Data Privacy Gap Assessment

SecureTrust will work with Client, through interviews, discussions and documentation review to identify critical people, processes and technology that support compliance with privacy regulation. The gap assessment process will identify gaps to achieving compliance with privacy regulation.

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 gap assessment results.

Outputs include:

- Gap matrix and corresponding recommendations.

Phase III: Reporting

SecureTrust will create, prepare and deliver to Client a report documenting all findings and recommendations from the assessment.

Outputs include:

- Data Privacy Gap Assessment Report to:
    - Document gaps identified by SecureTrust.
    - Provide recommendations to close identified gaps.

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 within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine gap assessment results.
- Create, prepare and deliver to Client a final report documenting findings and recommendations from the assessment.

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 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 assessment 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 assessment consists of remote and onsite activities.
- The assessment period 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 assessment.
- SecureTrust will perform the service in the English language.
- SecureTrust will not create or modify Client documentation as part of the Data Privacy Gap Assessment.
- SecureTrust will not provide remediation services as part of the Data Privacy Gap Assessment.
- SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Gap Assessment does not guarantee compliance with data privacy regulation. Client is responsible for making all management decisions with regard to its data privacy policies.
- SecureTrust does not offer a data privacy compliance guarantee. If Client is unable to demonstrate compliance with all requirements, the final report will be a gap analysis documenting the process and outcomes of the assessment.
- 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.