SecureTrust
a Trustwave division

Service Description

Data Privacy Risk Assessment

Contents

Data Privacy Risk Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Risk Assessment (the "Service") identifies the gaps against the privacy regulatory requirements specified in the applicable Order Form or SOW ("Privacy Requirements") and assesses the risks to personally identifiable information ("PII") or personal data processed within any internal or external business process, with recommendations on remediation for procedures, process, technology, and controls throughout business processes.

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 (GCRS)

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, responsible for conducting the assessment, reporting, and 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.

DPRA – The Services identifies risks to the protection of PII or personal data and compliance with Privacy Requirements. SecureTrust will provide Client with a final report documenting observations and recommendations.

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, technology, and data privacy management program.

SecureTrust's consultants will collect information from personnel in different levels of Client's organization with business and information technology expertise. SecureTrust will collect policies and procedures, data mappings, diagrams, and other related documentation to identify the risk profile of people, processes, and technology.

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.
- Engage with key management to understand Client's strategy, objective, scope and risk appetite.
- Review diagrams, data flows, and supporting documentation.
- Review business goals and strategic directions that impact the handling of PII or personal data.
- Review business operations including internally performed and outsourced processes that handle PII or personal data, including data brokers, controllers or processors if applicable, to understand and document their processing activities.
- Review key IT systems and their data privacy related documentation and configurations.
- Review key organizational documentation, including Client's policies and procedures.
- Review the applicable Privacy Requirements.

Phase II: Data Privacy Risk Assessment

SecureTrust will work with Client through documentation review, interviews, discussions, facilities inspections ,and controls analysis to conduct the Service. The Service will identify risks to the protection of PII and compliance with Privacy Requirements.

Key activities include:

- Conduct remote meetings and onsite visits.
- Confirm the critical assets including people, process and technology handling PII or personal data.
- Map privacy and security requirements across relevant internal policies and procedures.
- Review and analyze data actions on PII or personal data.
- Review and analyze IT system data privacy related capabilities.
- Catalog and analyze data actions on PII or personal data.
- Determine the risks to the protection of PII or personal data and compliance with Privacy Requirements .

- Assign risk values to all risks identified.
- Prioritize Risk from assessing potential impact and likelihood of occurrence
- Identify mitigating controls
- Document the Service results.

Phase III: Reporting

SecureTrust will develop a draft report documenting observations and recommendations from the assessment to establish a record of potential risks to PII or personal data including the potential likelihood and impact of risks. The draft report will be sent to Client for review. Client may comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide a final deliverable, including the final report and associated documentation, as defined below:

- A final report to:
    - Summarize the Service;
    - Document risks identified by SecureTrust; and
    - Provide recommendations to mitigate risk.

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, resource requirements and escalation procedures.
- 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 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 key steps, milestone dates, estimates for duration, deliverables, resource requirements and escalation procedures.

- Accurately provide all necessary information including key stakeholders, applicable environment information and configuration requirements.
- Inform SecureTrust of all 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.
    - 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 Controllers or Processors are involved.
    - The Service complements and does not replace Client ongoing internal data privacy risk assessment processes.
    - This Service assumes Client has identified and mapped data throughout the organization, lines of business, product, or service for which the Service is being conducted.
    - The Service consists of remote and/or onsite activities.
    - The start and end dates will be determined during the kickoff call.
    - SecureTrust may request evidence from Client's systems and processes as required to determine risk. 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.
    -