Service Description

Data Privacy Mapping

Contents

Data Privacy Mapping

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Mapping is a professional services engagement. Data Privacy Mapping is designed to facilitate the process of mapping data sources and associating data to identities. The Data Privacy Mapping service helps organizations address privacy and regulatory requirements.

BASE SERVICE FEATURES

SecureTrust's Data Privacy Mapping 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 (GCRS)

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 Data Privacy Mapping activity, reporting and consulting activities.

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.

Data Privacy Mapping – Consulting to identify the data sources and map the processes that support the reception, processing, manipulation, storing, and transmission of privacy data and personally identifiable information (PII). SecureTrust will assist Client in developing data maps and provide a high-level summary report to describe the process and outcomes of the data mapping activity.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the Data Privacy Mapping 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 Compliance Manager application for data sharing.

Outputs of the Project Initiation phase:

- 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 data privacy operations, data classification, data maturity, data handling and retention processes, and data ownership.

SecureTrust’s consultants will collect information from personnel in various levels of the organization as well as from those with business and information technology expertise.

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 facilitate the Data Privacy Mapping service and identify required documentation.
- Issue list of requested documents and meetings.
- Identify data map owners to provide information for the following:
    - Data input systems and logic that acts upon data
    - Database files, logs, and any other related repositories
    - Flat files from special action upon data
    - Data contained in in-direct processes such as logging and monitoring
    - Data contained in email systems, fax systems, traditional mail and other communication systems
    - Data Loss Prevention (DLP) tools
    - Intrusion Detection and Prevention System (IDS/IPS) repositories
    - Security Operations Center (SOC) log, filtering, or rule files
    - Network Operations Center (NOC) log, filtering, or rule files
    - Other hardcopy, analog or digital data stores
    - Other areas as identified and relevant to PII

Outputs of the Discovery phase include:

- Schedule of site visits, remote workshops and interviews.

Phase II: Data Privacy Mapping

SecureTrust will work with Client, through interviews, discussions and documentation review to assist Client in developing data maps that, identify, and categorize the data throughout its lifecycle for the following areas:

- Origination, transmission flows, storage points and 3rd party interactions with data as well as incidental data leaks connected to logging, monitoring, and data preservation activity.
- Origin of all PII data into the organization
- Internal data transmission paths
- External data transmission paths
- Data storage areas such as database, flat files and custom files
- External third-party data transfers
- Data contained in email systems, fax systems, traditional mail and other communication systems
- Logging and monitoring systems
- Data Loss Prevention (DLP) storage
- Backup systems and processes
- Decommissioned systems and drives
- Legal touch points (i.e., E-discovery systems)
- Other hardcopy, analog or digital data stores

Phase III: Reporting

SecureTrust will create, prepare and deliver to Client a report documenting findings and recommendations from the data mapping activity to establish a high-level data mapping of scoped and identified PII interactions.

Outputs of the Reporting phase include:

- Data map and/or data diagram.
- Summary report to describe process and outcome of the data mapping activity.

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, resource requirements and escalations procedures.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Create, prepare and deliver to Client a final report documenting findings and recommendations.

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, resource requirements and escalations 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 Data Privacy Mapping 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.
    - 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.
        - Privacy Officer or Data Protection Officer.
    - The project consists of remote and onsite activities.
    - The project start and end dates will be determined during the kickoff call.
    - SecureTrust is not responsible for defining systems in scope or whether information provided by Client is accurate.
    - SecureTrust will not provide remediation services as part of the Data Privacy Mapping
    - SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Mapping Service 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 this service is dependent on Client’s provision of accurate information and access to Client systems and resources to SecureTrust.