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 (DPRA) service is a professional services engagement. The DPRA identifies the gaps against a given requirement and assesses the risks to personal data processed within any internal or external business process, with recommendations on remediation for procedures, process, technology and physical controls throughout business processes. The DPRA helps organizations measure risk and facilitate senior management endorsement and cross-functional collaboration to manage risk treatment for key privacy and security risks using relevant controls.

BASE SERVICE FEATURES

SecureTrust's DPRA service 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 serves as the primary resource for the fulfilment of the service, responsible for performing the risk assessment, reporting and assisting Client in remediation planning regarding how personal data is captured, stored, maintained and protected.

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.

DPRA – An assessment of risks to personal data processed throughout Client business processes. A SecureTrust Security Consultant works with Client to carry out a review of information, assets, processes and interview resources to gather information for analysis, enabling SecureTrust to carry out a comprehensive risk assessment and produce an actionable report and a risk register that can be used stand-alone or may be imported into Client's risk register.

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 escalation procedures.

SecureTrust will work with Client to identify relevant business environments, procedures, processes, systems, and controls which should be assessed during the assessment.

Project Initiation activities include:

- Introduction to the SecureTrust Compliance Manager application for data sharing.
- Issuing list of requested documents and meetings to understand the scope of the engagement.

Outputs of Project Initiation activity includes:

- Agreement on the project scope and expected deliverables
- Commitment to regular project status meetings with key stakeholders
- Agreement on project plan, stakeholders as well as roles and responsibilities.

Phase I: Organizational Review and Assessment Data Discovery

SecureTrust will interview appropriate personnel, including third parties as required, to understand the details of the organization's operations; data classification, data maturity, data handling and retention processes, and data ownership. Interviews include a series of knowledge interviews. SecureTrust's consultants will collect information from personnel in different levels of the organization as well as from those with business and information technology expertise. Each knowledge 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 (senior management, operational area management and other staff both business and information technology personnel).

Key activities include:

- Schedule a site visit or remote workshop to facilitate the scoping of the assessment and identify required documentation.
- Engage with key management to understand Client's strategy, objective, scope and risk appetite.
- Remotely review diagrams, data flows, and documentation and confirm scope of the assessment.
- Understand business goals and strategic directions that impact the handling of personal data.
- Review business operations including internally-performed and outsourced processes.
- Review Key IT systems and their security-related documentation/ configuration.
- Key organizational documentation, including Client's policies and procedures.
- Review and understand the applicable privacy regulatory requirements.

Outputs include:

- Confirmed scope statement including summary of key business units, activities and high level data-flows.
- Agreed risk assessment methodology, matrix and template.

Phase II: Assess Risk of Personal Data

Critical people, process and technology assets that are operated and managed internally and outsourced are defined based on Phase I outputs. The risk assessment process will identify and assess the associated risk factors and existing controls against a list of integrated, mapped requirements.

Key activities will include:

- Conduct remote meetings, onsite visits, interviews and discussions as identified in Phase I.
- Conduct one to one interviews.
- Process procedural reviews.
- Confirm the critical assets (including people, process and technology handling privacy data).
- Map privacy and security requirements across relevant internal policies and procedures.
- Analyze data provided and captured in order to assess technological risks.
- Determine the risks to the protection of personally identifiable information (PII) or compliance with laws arising from data processing or individuals' interactions with systems, products, or services.
- Assign risk values to all risks identified.
- Prioritize Risk from assessing potential impact, likelihood or occurrence
- Identify mitigating controls
- Document the risk assessment results.

Outputs will include:

- A populated and prioritized risk register with potential mitigation strategies and recommendations.
- Control gap matrix with gap description and corresponding risks.

Phase III: Reporting

SecureTrust will create, prepare and deliver to Client a report documenting all findings and recommendations from the assessment to establish a record of potential risks regarding the confidentiality and integrity of personal data processes within the Client organization and its suppliers.

The following documents and content will be included in the final deliverables:

- An executive report, supported by outputs from previous phases, which includes a summary of:
    - Scope and approach
    - A descriptive assessment and relative risk score from each risk category in all areas considered.
    - Risks identified by SecureTrust with risk mitigation recommendations.
    - Recommended solutions and specific additional controls recommendations.

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 escalation procedures.
- 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.
- Interview appropriate organization personnel and collect information from personnel.
- Determine risk assessment results.
- Create, prepare and deliver to Client a final report documenting all 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 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 risk assessment 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.
    - SecureTrust's DPRA methodology is based on industry standards including International Organization for Standardization (ISO) 31000: 2018 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 , and NIST SP 800-122. The proposed methodology is data privacy focused, and not solely meant to conform to a single standard. Other standards may be used to facilitate the assessment.
    - The service complements and does not replace the Client internal gap, and/or risk assessment process.
    - 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 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 will not create or modify Client documentation as part of the Data Privacy Risk Assessment.
- SecureTrust will not provide remediation services as part of the Data Privacy Risk Assessment.
- SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Risk Assessment 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.