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) 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.

BASE SERVICE FEATURES

SecureTrust's DPRA 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 conducting 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 as well as serves Client as a secondary point of contact for escalations and queries.

DPRA – An assessment to identify risks to the protection of personally identifiable information and comply with privacy laws and regulations. A SecureTrust security consultant will work with Client to conduct a comprehensive data privacy risk assessment. SecureTrust will produce a data privacy risk assessment report documenting findings and recommendations.

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.

Key activities include:

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

Outputs 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, process and technology.

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 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 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.
- Review 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 dataflows.
- Mutually agreed risk assessment methodology, matrix and template.

Phase II: Risk Assessment

SecureTrust will work with Client, through interviews, discussions and documentation review to conduct a data privacy risk assessment. The risk assessment process will identify risks to the protection of personally identifiable information and compliance with privacy laws and regulations

Key activities include:

- Conduct remote meetings and onsite visits to facilitate interviews, discussions and documentation review.
- 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 risk
- Determine the risks to the protection of PII and compliance with privacy laws and regulations.
- Assign risk values to all risks identified.
- Document the risk assessment results.

Outputs include:

- A populated risk register in a mutually agreed upon format.

Phase III: Reporting

SecureTrust will create, prepare and deliver to Client a report documenting findings and recommendations from the assessment to establish a record of potential risk regarding the confidentiality and integrity of personally identifiable data processes.

Outputs include:

- A Data Privacy Risk Assessment Report to:
    - Document risks identified by SecureTrust
    - Provide recommendations to mitigate risk.

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 within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine data privacy risk 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 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 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.
    - 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 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 assessment.
    - SecureTrust will not create or modify Client documentation as part of the DPRA.
    - SecureTrust will not provide remediation services as part of the DPRA.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the DPRA 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.
    - This service assumes client has identified and mapped data throughout the organization, lines of business, product, or service for which the risk assessment is being conducted. If not, then client will need to complete this step.