SecureTrust
a Trustwave division

Service Description

California Consumer Privacy Act Gap Assessment

Contents

CCPA Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's California Consumer Privacy Act (CCPA) Gap Assessment is a professional services engagement. The CCPA Gap Assessment is designed to identify gaps to achieve compliance with the CCPA.

BASE SERVICE FEATURES

SecureTrust's CCPA Gap Assessment includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application which manage the engagement process and collects and securely stores 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 CCPA Gap Assessment, compliance determination and reporting.

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.

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

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate successful 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. 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, key steps, assessment dates, stakeholders as well as roles and responsibilities.

Phase I: 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. 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 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 and 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.

SecureTrust will begin report deliverable development.

Phase II: CCPA Gap Assessment

SecureTrust will work with Client, through interviews, discussions and facilities inspections to identify critical people, processes and technology assets that are operated and managed internally and outsourced. The gap assessment process will identify and assess existing controls.

Key activities include:

- Remote meetings and onsite visits to conduct interviews and discussions.
- Process procedural reviews.
- Confirmation of 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 gaps.
- Document the gap assessment results.

Outputs include:

- Control gap matrix and corresponding recommendations.

SecureTrust will continue development of the report deliverable.

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 gaps regarding the confidentiality and integrity of personal data processes within the Client organization and its suppliers.

Outputs include:

- Gaps identified by SecureTrust.
- 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 in accordance with the CCPA.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.
- Conduct closeout meeting.

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.
- 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.
- 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 gap assessment activities in relation to Client's environment.
- 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 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 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 CCPA Gap Assessment.
    - SecureTrust will not provide remediation services as part of the CCPA Gap Assessment.
    - For any services or validation requirements identified during the course of the assessment that are not directly included in the pricing table, Client must separately contract for the additional services or validation efforts as an addendum to this agreement.