

Service Description

National Institute of Standards and Technology

Privacy Framework Consulting

Contents

National Institute of Standards and Technology (NIST) Privacy Framework Consulting	3
Service Description	3
Base Service Features	3
SecureTrust® Portal	3
Global Compliance and Risk Services (GCRS)	3
Delivery and Implementation.....	3
Project Initiation	3
Phase I: NIST Privacy Consulting	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES.....	4

National Institute of Standards and Technology (NIST)

Privacy Framework Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's National Institute of Standards and Technology (NIST) Privacy Framework Consulting is a professional services engagement. NIST Privacy Framework Consulting is designed assist and guide organizations in gaining an understanding of and adopting the NIST Privacy Framework.

BASE SERVICE FEATURES

SecureTrust's NIST Privacy Framework Consulting 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 fulfillment of the service, responsible for performing the NIST Privacy Framework Consulting activity.

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.

SecureTrust's (NIST) Privacy Framework Consulting – Consulting services to assist and guide Client to adopt the NIST Privacy Framework. The Security Consultant will provide Client with assistance and guidance to adopt the NIST Privacy Framework.

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

Project Initiation activities include:

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

Outputs for the Project Initiation phase:

- Agreement on the high-level project plan
- Regular project status meetings with key stakeholders

NIST Privacy Consulting

SecureTrust will work with client to provide assistance and guidance to responsible privacy personnel on how to use the framework in the context of any privacy laws, regulations or business requirements. SecureTrust consultant will then work with the identified personnel to adopt the framework into the organization.

Key activities include:

- Identify Client privacy stakeholder or business owner responsible for the privacy program and/or adoption of the NIST Framework.
- Review the critical components of the NIST Privacy Framework in the context of the laws, regulations or business requirements to which Client is subject.
- Review existing data protection strategies.
- Engage with key management to understand Client's strategy, objective, scope and risk appetite.
- Understand business goals and strategic directions that impact privacy.
- Define with the client the key aspects of the NIST Privacy Framework (Core, Functions, Profiles).
- Assist client with use and adoption of NIST Privacy Framework and data protection strategies for processing, storing, transmitting, and sharing with third parties.

Outputs include:

- Client knowledge, skill and ability to adopt the NIST Privacy Framework Plan.
- Summary report to describe process and outcome of the NIST Privacy Consulting activities.

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 and escalation procedures.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Interview appropriate organization personnel and collect information from personnel.

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 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 risk assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
 - 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 brokers, controllers or processors.
 - Privacy Officer or Data Protection Officer.
 - The consulting engagement consists of remote and onsite activities.
 - The consulting engagement starts 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 perform the service in the English Language.
 - SecureTrust will not create or modify Client documentation as part of the NIST Privacy consulting.
 - SecureTrust will not provide remediation services as part of the NIST Privacy consulting.
 - SecureTrust will not offer any legal guidance or counseling. The provision of NIST Privacy Consulting 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.