

Service Description

National Institute of Standards and Technology

Controls Assessment

Contents

NIST Controls Assessment	3
Service Description	3
Base Service Features	3
SecureTrust Portal.....	3
Global Compliance and Risk Services	3
Delivery and Implementation.....	3
Project Initiation	3
Phase I: Discovery.....	4
Phase II: Security Controls Assessment	4
Phase III: Reporting.....	4
SECURETRUST RESPONSIBILITIES	4
CLIENT RESPONSIBILITIES.....	5

NIST Controls Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Security National Institute of Standards and Technology (NIST) Controls Assessment is a professional services engagement. The NIST Controls Assessment is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with a subset of NIST Special Publication (SP) 800-53, Revision Four controls.

The NIST Controls Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection and review of security architecture.

BASE SERVICE FEATURES

SecureTrust's NIST Gap Assessment 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

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Security Consultant – An information security consultant and is the primary resource for the fulfilment of the service, responsible for conducting the onsite assessment, compliance determination and reporting.

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.

NIST Controls Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with a subset of NIST SP 800-53, Revision Four controls.

SecureTrust will provide Client with a NIST Controls Assessment. SecureTrust will provide a report detailing the results of the NIST Controls Assessment.

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.

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of the controls environment.

Phase I: Discovery

SecureTrust will work with Client, where applicable, to:

- Determine critical assets;
- Examine business processes;
- Identify security and compliance management processes in place; and
- Review previous compliance or assessment documentation.

Phase II: Security Controls Assessment

SecureTrust will work with Client through interviews, discussions, and facilities inspections to:

- Ensure Client has adequate knowledge about NIST requirements and responsibilities of all parties involved to demonstrate NIST compliance;
- Ensure assessor has knowledge of environment to identify critical gaps between Client's current state and NIST requirements;
- Identify critical gaps between security activities for the NIST Controls Assessment report to enumerate gaps;
- Gain reasonable assurances of Client compliance posture; and
- Prioritize remediation efforts required to achieve compliance.

Phase III: Reporting

SecureTrust will:

- Analyze evidence against applicable NIST requirements;
- Determine Client's compliance posture; and
- Deliver the NIST Controls Assessment report.

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.
- Perform controls assessment against the applicable NIST control testing procedures.
- Provide Client with information on any findings that requires remediation.
- Determine NIST Controls Assessment results and Client's status.

- Produce a NIST Controls Assessment report on the status of the solution, component or application at the time the assessment occurs.
- 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 client environment information and configuration requirements.
- Inform SecureTrust of all Client 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 compliance 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.
 - The assessment consists of both onsite and remote assessment 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 service.
 - SecureTrust will perform the service in the English language.
 - SecureTrust will not create or modify Client documentation as part of the NIST Controls Assessment.
 - SecureTrust will not provide remediation services as part of the NIST Controls Assessment.
 - SecureTrust will not offer any legal guidance or counseling.
 - 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.