

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.....	4
Project Initiation	4
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 (the "**Service**") 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 Five controls.

SecureTrust evaluates Client's policies, procedures, and practices through documentation review, interviews, discussion, facilities inspection, and controls analysis.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at <https://www.trustwave.com/en-us/legal-documents/contract-documents/> or a similar agreement signed between SecureTrust and Client.

BASE SERVICE FEATURES

The Service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal features consist of, among others, 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 – A Security Consultant and is the primary resource for the fulfilment of the NIST Controls Assessment, responsible for conducting the assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the Security Consultant and serves as Client's secondary point of contact for escalations and queries.

NIST Controls Assessment – An assessment that identifies gaps and aims to prioritize areas that may require remediation to achieve compliance with a subset of NIST SP 800-53, Revision Five controls. SecureTrust will provide a final report detailing the results of the NIST Controls Assessment.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by scheduling and conducting a 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.

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 may conduct interviews, discussions, and facilities inspections to:

- Evaluate Client's knowledge about NIST requirements and responsibilities of parties involved;
- Become familiar with Client's environment to identify critical gaps between Client's current state and NIST requirements;
- Prioritize remediation efforts that may be required to achieve compliance.

SecureTrust will analyze the results of the assessment activities in the context of NIST 800-53, Revision Five and industry best practices, as determined applicable by SecureTrust.

Phase III: Reporting

SecureTrust will develop a NIST Controls Assessment Report identifying areas of non-compliance. The NIST Controls Assessment Report includes details of non-compliant observations and may recommend specific changes that may bring Client's environment into compliance with NIST 800-53, Revision Five.

The draft NIST Controls Assessment Report will be sent to Client. Client may comment and suggest changes to the draft report with supporting documentation. The SecureTrust QA team will finalize the draft report. SecureTrust retains final authority regarding the contents of the NIST Controls Assessment Report.

SecureTrust will provide a final NIST Controls Assessment Report.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from 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.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.

- Interview appropriate Client personnel and collect information from personnel.
- Identify to Client observations that may require remediation.
- Produce a draft NIST Controls Assessment Report.
- Deliver to Client a final NIST Controls Assessment Report documenting observations and recommendations from the Service.

CLIENT RESPONSIBILITIES

- Establish contact and remain available for communications from 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 the Service 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 Service may consist of onsite and remote assessment activities.
 - The Service 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 Service.
 - SecureTrust will not provide remediation services as part of the NIST Service.
 - 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.