SecureTrust
a Trustwave division

Service Description

International Organization for Standardization

Gap Assessment

Contents

ISO Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Internal Organization for Standardization (ISO) Gap Assessment (the "**Service**") is designed to help identify gaps and prioritize areas that may require remediation to achieve compliance with ISO 27001/2:2013 controls.

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 is Client's primary resource during the Service and is responsible for conducting the assessment, evaluating compliance, and producing the report.

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.

ISO Gap Assessment – The Service aims to identify gaps and prioritize areas that may require remediation to achieve compliance with ISO 27001/2:2013 controls.

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: Information Gathering

SecureTrust will work with Client to determine critical assets, examine business processes, and identify security and compliance management processes in place. SecureTrust will work with Client, where applicable, to collect documentation and evidence including but not limited to:

- Policies and procedures;
- Asset inventories;
- Architectural drawings;
- Data flow diagrams;
- Network diagrams; and
- Other security management documentation which defines the Client environment.
- Review Client environment and organization, including related security management documentation.
- Identify action items or missing information.

Phase II: ISO Gap Assessment

SecureTrust may use documentation review, interviews, discussions, facilities inspection, and controls analysis to conduct the Service.

Key activities include:

- Confirm ISO domains and controls in scope;
- Review security policies, processes, guidelines;
- Review asset inventories, architectural drawings, data flow and network diagrams;
- Review existing Client controls against the ISO 27001/2:2013 standard(s):
    - Determine whether Client controls satisfy, partially satisfy, or do not satisfy the ISO 27001/2:2013 standard for the designated ISO domains.

SecureTrust will review in the context of ISO 27001/2:2013 and industry best practices, as applicable.

Phase III: Reporting

SecureTrust will develop an ISO Gap Assessment Report to identify areas of non-compliance with ISO 27001/2:2013 pertaining to Client's environment. The ISO Gap Assessment Report includes details of non-compliant observations and may recommend specific changes to bring Client's environment into compliance with the ISO 27001/2:2013 standard.

SecureTrust will send a draft ISO Gap Assessment Report to Client. Client may comment and suggest changes to the draft report with supporting documentation. The SecureTrust QA team will review and suggest changes to finalize the draft report. SecureTrust retains final authority regarding the contents of the final ISO Gap Assessment Report.

SecureTrust will provide a final ISO Gap 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.
- Assess compliance of the ISO domains and controls in scope;
- Respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate Client personnel and collect information from such personnel as needed.
- Determine assessment results.
- Identify to Client observations that may require remediation.
- Produce a draft ISO Gap Assessment Report.
- Deliver to Client a final ISO Gap 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 compliance 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.
    - SecureTrust is not a certifying body for the purposes of issuing compliance certificates for the ISO 27000 series.
    - The Service may consist of remote and onsite 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 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.