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 is a professional services engagement. The ISO Gap Assessment is designed to help identify gaps, and prioritize areas that may require remediation, to achieve compliance with an organization's implementation of ISO 27001/2:2013 controls to aid in implementing security best practices.

## BASE SERVICE FEATURES

SecureTrust's ISO Gap Assessment service 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 is the primary resource for the fulfilment of the service, responsible for performing the compliance 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.

Gap Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with an organization's implementation of ISO 27001/2:2013 controls. SecureTrust will provide Client guidance for design of controls and identification of supporting organizational policy, procedures and practices. SecureTrust will provide an ISO Gap Assessment Report.

## 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.

## Phase I: Discovery

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 environment.
- Review environment and organization, including related security management documentation.
- Identify action items or missing information.

SecureTrust will begin report deliverable development.

## Phase II: Gap Assessment

SecureTrust will work with Client, through interview, discussion and facilities inspections to assess:

- ISO domains and controls;
- Security policies, processes, guidelines;
- Asset inventories, architectural drawings, data flow and network diagrams;
- Existing Client controls against the ISO 27001/2:2013 standard(s) to determine:
    - Whether Client controls satisfy, partially satisfy, or do not satisfy the ISO 27001/2:2013 standard for the designated domains.

SecureTrust will provide preliminary comments, findings and recommendations, as needed, to Client point of contact to support evaluation ratings.

SecureTrust will continue report deliverable development.

## Phase III: Analysis

SecureTrust will analyze findings from the high level assessment in the context of ISO 27001/2:2013 and industry best practices, as applicable.

SecureTrust will continue report deliverable development.

## Phase IV: Reporting

SecureTrust will analyze evidence in accordance ISO standards, determine Client compliance status and complete development of the report deliverable.

SecureTrust will:

- Review a draft report with Client point of contact.
- Perform one revision of the report, if required.
- Deliver the final ISO 27001/2:2013 Gap Assessment Report to Client point of contact.
- Conduct review of final report with Client management team, if required.

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.
- Confirm the ISO domains and controls in scope;
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine gap assessment results.
- Create, prepare and 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.
    - SecureTrust is not a certifying body for the purposes of issuing compliance certificates for the ISO 27000 series.
    - The engagement consists of remote and onsite 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 ISO Gap Assessment.
- SecureTrust will not provide remediation services as part of the ISO Gap 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.