SecureTrust
a Trustwave division

Service Description

Information Security Risk Assessment

Contents

Information Security Risk Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Information Security Risk Assessment (ISRA) (the "**Service**") helps Client understand assets, vulnerabilities, threats, likelihood of threat events in, and impact of threat events on Client's information security environment. The Service helps Client measure risk and plan risk mitigation measures.

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 (GCRS)

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

Security Consultant – A Security Consultant serves as Client's primary resource during the Service and is responsible for conducting the assessment 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.

ISRA – An assessment of threats, vulnerabilities, likelihood of threat events in, and impact of threat events on Client's information security environment with its existing security controls. A Security Consultant will work with Client to conduct a comprehensive risk assessment and produce a report documenting observations and recommendations.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by 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: Information Gathering

SecureTrust will work with the Client to understand their business processes and the current controls as relate to key information assets within Client's environment. SecureTrust and Client will work to identify relevant key assets, business environments, procedures, systems, and controls to be assessed as a part of the Service. SecureTrust may request information on the following:

- Key IT systems;
- Logical and physical access controls;
- Information classification and handling policy;
- Third party service provider management; and
- Incident response management.

SecureTrust may consider conditions in Client's environment that could increase or decrease the likelihood of threat events or impact on assets. If available, SecureTrust may use information from previous audits, security assessments, vulnerability scans, penetration tests, code reviews, and any other relevant documentation.

Phase II: Information Security Risk Assessment

SecureTrust will interview appropriate personnel from appropriate levels and functions within Client's organization to understand the details of the business operations and complete the following activities:

- Identify assets and relative priorities of each;
- Identify threat and risk areas;
- Identify 'current state' security for priority assets; and
- Identify current security practices and organizational objectives.

During the interview sessions, SecureTrust seeks to identify de facto practices that may benefit from being formalized in written policy.

SecureTrust will examine key components of Client's information technology infrastructure to determine technology or process vulnerabilities in the following control groupings:

- Communication security controls
- Endpoint security controls
- Protective monitoring controls
- IT threat management controls
- Security governance controls

SecureTrust will perform an on-site assessment of Client's facility including computer rooms, communications facilities, physical security facilities and systems, and any other relevant aspects of the operational environment.

SecureTrust will apply threat scenarios based on sources of risk agreed between SecureTrust and Client to determine the likelihood and impact of known or hypothesized outcomes. From these threat scenarios, the most critical assets will be assigned a threat profile for relative weighting within the overall risk calculation.

The level of risk is calculated by comparing:

- Likelihood of a threat exploiting a vulnerability; and
- Severity of impact that the exploited vulnerability would have on the system, data and function in terms of loss of confidentiality, integrity or availability.

SecureTrust will analyze Client's environment in the context of end-to-end processes and existing controls. Client and SecureTrust will conclude this phase by agreeing on what may require additional review and corrective action planning.

Phase IV: Reporting

SecureTrust will develop an ISRA Report documenting observations and recommendations from the Service as a record of potential risks to critical assets.

The draft ISRA 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 final ISRA Report.

SecureTrust will provide, as the final deliverable for the Service, an ISRA Report which includes:

- Documentation of risks identified by SecureTrust
- Recommendations for mitigation of such risks.

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.
- Validate scope of the ISRA.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine ISRA compliance results.
- Provide Client with information on any observations that require remediation.
- Produce a draft ISRA Report.
- Deliver to Client a final ISRA 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 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 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.
    - Client's personnel from the following departments will typically need to be involved:
        - Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
    - SecureTrust's risk assessment methodology is based on industry standards current as of the Service start date including International Standard Organization (ISO) 27000 series, National Institute of Standards and Technology (NIST) Special Publication 800-30 and Operational Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Other standards may be used to facilitate the Service as determined by SecureTrust relative to the size, complexity, and needs of the Client.
    - The Service complements and does replace Client's ongoing internal risk assessment processes.
    - The Service may consist of both 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.