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) is a professional services engagement. The ISRA helps organizations gain an understanding of assets, vulnerabilities, threats, likelihood of threat events, and impact of threat events on their information security environment. The ISRA helps organizations measure risk and plan risk treatment.

BASE SERVICE FEATURES

SecureTrust's ISRA 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 (GCRS)

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

Security Consultant – An information security consultant serves as the primary resource for the fulfilment of the service, responsible for performing the risk assessment and reporting.

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

ISRA – A risk assessment of threats, vulnerabilities, likelihood of threat events, and impact of threat events on a Client's information security environment given existing security controls. A SecureTrust Security Consultant will work with Client to gather information for analysis, conduct a comprehensive risk assessment and produce an actionable report that may be imported into Client's risk register.

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: Organizational Review and Discovery

SecureTrust will work with the Client to understand their business processes and the current controls as they relate to key information assets within the Client environment. SecureTrust will work with Client to identify relevant key assets, business environments, procedures, systems, and controls to be assessed during the assessment. SecureTrust will request information including, but not limited to:

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

SecureTrust will include consideration of predisposing conditions in Client's environment that will increase or decrease the likelihood of threat events or impact on assets. When available, SecureTrust will leverage input from previous audits, security assessments, vulnerability scans, penetration tests, code reviews and any other relevant documentation that may be made available.

Phase II: Risk Assessment

SecureTrust will interview appropriate personnel from all appropriate levels and functions within the organization to understand the details of the business operations in order to elicit the following:

- Identification of assets and relative priorities of each;
- Identification of 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 determine any de facto practices being followed that should be formalized in written policy.

SecureTrust will examine the 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 agreed sources of risk and determine the likelihood and impact of the known or hypothesized outcomes. From these scenarios, the most critical assets will be assigned a threat profile for integration and relative weighting, with the overall profile.

Phase III: Risk Analysis

SecureTrust will analyze all the information captured to determine risks to critical assets.

The level of risk is calculated based on:

- 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.

Findings and guidance will be analyzed against the context of end-to-end processes and existence of existing controls. The end result will be an agreement on those findings that require attention, and corresponding corrective action planning.

Phase IV: Reporting

SecureTrust will create, prepare and deliver a report to Client documenting all findings and recommendations from the assessment to establish a record of potential risks to critical assets. The risk assessment report will include the following:

- Overall risk ranking relative to data classification;
- Detailed breakdown of security control gaps; and
- Recommendations for risk mitigation

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.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine risk 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 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 risk assessment activities in relation to Client’s environment.

- 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.
    - Personnel from the following departments are generally 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 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 assessment as determined by the size, complexity and needs of the Client.
    - The service complements and does replace Client's ongoing internal risk assessment processes.
    - The assessment consists of both 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 Information Security Risk Assessment.
    - SecureTrust will not provide remediation services as part of the Information Security Risk 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.