SAPPHIRE™

Corporate Security Awareness Review Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

In today's Information Age, companies understand the importance of information security and the impact it has on their company's ability to trade, deliver key operational services, protecting customer data and trust, make profit, optimise performance and affect their future growth. Information security is based on ensuring the appropriate and commensurate controls as in place to protect the Confidentiality, Integrity and Availability of both corporate and customer Information, in line with the risk appetite of the company. Sapphire incorporates a Risk Management approach towards the physical, procedural, people and technical aspects associated to the key business processes of our client's business. Our Corporate Security Awareness Report provides a comprehensive security improvement plan to ensure key information assets are protected from breaches or disaster, while authorised staff can access corporate information from wherever and whenever the business needs to.

Functional and Non-Functional Detail

Sapphire's approach to providing our Corporate Security Awareness Report (CSAR) is based on the following steps:

1. Scoping
2. Business Review
3. Gap & Risk Analysis
4. Corporate Security Awareness Report

Business Review

Understanding your business is critical to ensure the security measures are appropriate and commensurate to the business requirements of the company. During this phase Sapphire require to understand the following areas:

- Business Objectives
- Business processes
- Compliance requirements
- Existing security culture

The strategic Business Objectives will be defined during the initial meeting with the Project Sponsor.

The key Business Processes, within the scope of the security review, will be analysed to identify any potential areas of weakness in relation to the confidentially, integrity and availability of the individual activities the business process provides and/or relies upon.

External and internal Compliance requirements will be discussed and any key areas included into the Gap Analysis review phase.

A review of the existing security culture and security maturity will be conducted by Sapphire to understand the level of security controls and good practices that have been successfully adopted and integrated into your company.

Client requirement: This phase would require meetings with staff who are responsible for and understand the key business processes within the scope of this project. Each key process meeting is expected to last about 2 hours per process. However, if the processes are integrated than a workshop would be scheduled for all interested parties to minimise staff involvement.

Gap and Risk Analysis

Gap Analysis

The Gap Analysis is a review of the current security practices within your business in line with recognised International Good Practice Guides, for Information Security (ISO 27001), Business Continuity Management (ISO 22301) and Supply Chain Management (ISO 27036).

Risk Assessments

Sapphire will carry out an Information Security Risk Assessment, which identifies the appropriateness of your existing security controls in relation to the value of the information asset/process it is protecting. Sapphire's Risk Assessment Methodology provides a prioritised list of Risks to your company assets.

The outcome of the Gap Analysis and Risk Assessment provides an 'as-is' picture of your current posture, in relation to the adoption of good security practices that are appropriate to the business objectives of the company.

Client Involvement: During this phase Sapphire analyses what security controls are in place including the Physical, Process, People and technical aspects of the systems with scope. It is expected that these would be approx. 45 Minute minutes with HR, Facilities, Legal, and Procurement. The meeting with IT to discuss technical controls is expected to last about half a day.

It should be noted that there may be follow up meetings with key staff to verify our findings and/or to discuss some area in more depth.

Corporate Security Awareness Report (CSAR)

Once we understand the 'as-is' position of the information security aspects of your company, we work with you to develop your Security Improvement Plan that identifies a clear plan of action for the implementation of security controls to allow you to meet your business objectives and implement good practice.

Your Corporate Security Awareness Report provides you with full details of our findings and a clear prioritised roadmap and action plan on how to achieve your goals ('to-be' plan) in relation to incorporating good information security practices within your business processes aligned to your risk landscape.

The Corporate Security Awareness Report is a security review of your company and comprises:

- An Executive Summary
- Business Overview
- Gap Analysis (with Statement of Applicability - where relevant)
- Risk Assessment
- Risk Treatment Plan
- Analysis of findings ('as-is')
- Security Improvement Plan ('to-be')

Sapphire's Certifications and Associations