1 Background

Stonebridge Consulting Ltd. (SC) works within an intensely competitive market wherein there are a significant number of IT consulting companies fighting for a relatively small share of the market. The company offers services in 3 main areas:

a. Cybersecurity, including cybersecurity assessments, programme development and maintenance and education of company executives

b. Security of Assets and People, including comprehensive security evaluations, integrated risk, vulnerability and threat assessments and equipment and technical infrastructure evaluation; and

c. Business Intelligence, including strategic intelligence, enhanced due diligence and world-wide asset tracing.

SC reported a turnover of £3 million in the financial year 2019-2020.

There are 5 departments (Consulting – by far the largest, sales, marketing, HR and IT) each led by a director. These departments are located in two offices in the UK, one in Silverstone and another in Cheltenham. Consulting staff along with Sales are based in Cheltenham. The Silverstone office houses the human resources, finance/purchasing and marketing departments. SC outsources its IT to CyHelm, an IT firm out of West London.

You are the Chief Information Security Officer (CISO) of SC. You report directly to the CIO. You have also been assigned to appoint a new Data Protection Officer, currently interviewing candidates.

The COVID-19 pandemic and the requirement for most organisations to change their modus operandi to remote working has led to a spike of high-profile cyber incidents, resulting in digital services outages which have attracted media attention. SC also has to comply with UK requirement to gain the Cyber Essentials Plus Certification in order to participate in Department of Defence projects. These two issues have led SC’s board of directors to take a highly radical approach to security.

There is now an overwhelming need to assess the risk for these two issues; risks of remote working and risks related to the activities required to be undertaken in order to achieve the Cyber Essential + accreditation. The board has suggested that the company should establish an information risk management strategy, commencing from a thorough risk assessment.

The members of the board have heard that capability maturity models provide holistic, enterprise level risk assessments. The CIO has asked you to review existing capability maturity models and provide a report outlining the model you believe is more applicable to SC while analysing how it should be applied within the company.

Executive Summary:

The report is intended for the consumption of the board members of SC. Thus, an Executive Summary, of no more than 2 pages must be included at the beginning of the Report.

Part A: Review

Capability maturity models for Information or Cyber Security, such as the Cybersecurity Capability Maturity Model[1], are tools for evaluating an organisation’s cyber/information security posture while illustrating organisational progression.

In the first part of the report you are required to provide a literature review of existing capability maturity models (this may include summarising the features of each model, the business areas it addresses and the assessment methodology it uses) and explain which model you recommend should be applied within SC.

Part B: Organisational Risk Landscape

Write a section which:

1. Identifies the risks related to remote working of staff for your corporate environment.

2. Identifies the risks related to the activities required to be undertaken in order to achieve the Cyber Essential Plus certification.

3. Describes the process for the implementation of the model within SC.

4. Explains why the recommended model is suitable to address the risks identified in the previous section.

[1] https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0