[Insert Report Title Here]

Course Code: [Insert course code]
Student Name: [Insert your name]
Student Number: [Insert your student number]
Submission Date: 5 October 2025
Word Count: [Insert approximate word count]

This assessment applies the CORAS methodology to analyse the risks of a SIM-porting attack on a home-based business. All information herein is fictional and for academic purposes only.

Executive Summary

Provide a concise overview of the scenario, the major risks you identified, and the most important recommended treatments. Limit this section to one paragraph.

1 Introduction

1.1 Problem Statement

Describe the backstory of your chosen home-based business. Outline the business model, the key technologies it relies upon (e.g., desktop computer, smartphone, online storefronts, IoT devices) and how a SIM-porting attack impacted operations.

1.2 Purpose and Objectives

State the aim of the risk assessment. Explain why you will use the CORAS methodology to identify and model risks, how you will assess their likelihood and impact, and propose treatments that align with best practice and relevant regulations. Clarify that your analysis will consider both technical and human factors and will be informed by credible external sources and regulatory guidance.

1.3 Target Description and Views

Describe the goals of the analysis, the specific target in use (e.g., the business's mobile number used for multifactor authentication, the online storefront, cloud services) and provide the business or organisation's views of these targets. Explain why these targets are important for the organisation and how the chosen scope reflects the business priorities.

1.4 Scope

Define which assets, processes and parties are in scope for your analysis (e.g., business devices, cloud services, telecommunications provider). Note what is out of scope (e.g., internal workings of third-party providers) and justify your choices.

1.5 Methodology and Standards

Briefly describe the CORAS approach and any other standards you reference (such as ISO 27005, NIST SP 800-30, ACMA or CISA guidance). Mention the tools you used to create diagrams (CORAS Editor, Visio, Draw.io, etc.).

2 Stakeholder and Viewpoint Analysis

Create a table summarising the stakeholders and their priorities. An example structure is provided; **add and/or modify** the rows to match your scenario.

Role / Viewpoint	Interest / Responsibility	Priority
Owner	[Describe business continuity, financial viability, protection of data, etc.]	H
Telecom Provider	[compliance with regulations,....]	[...]
Regulators	[...]	M
Any other stakeholder	[...]	[...]

3 Asset Identification and Valuation

3.1 Asset Relative Value Table

Provide a table of assets and assign relative values for confidentiality (C), integrity (I) and availability (A). Rank the assets based on their overall importance to the business. Include a brief note explaining why each asset is important. These rankings will feed into your TVA matrix in the risk analysis.

3.2 Asset Diagram

Insert your CORAS asset diagram here. Use CORAS symbols to represent the assets and show their relationships.

4 High-Level Threat Identification

Summarise the main threat agents, unwanted incidents and vulnerabilities relevant to SIM porting. Keep it high level; detailed modelling belongs in the threat diagram section.

5 Detailed CORAS Threat Diagram

Provide a detailed threat diagram showing **at least** two attack paths (i.e., unwanted incidents resulting in a threat-vulnerability entity in affecting one or more assets). Use CORAS notation and indicate the likelihood on each path where possible. Insert your diagram.

6 Risk Analysis

Explain your method for calculating likelihood and impact. Define a 1–5 impact scale appropriate for a microbusiness and justify your choices. Include a **Threat–Vulnerability–Asset (TVA) ranking matrix** that combines the importance of assets with the severity of threats and the existence of vulnerabilities to produce a ranked list of risks. Describe the risk function you use (for example, risk = likelihood $\times$ impact) and how you derive risk evaluation metrics. The TVA matrix need to help in visualise the severity of each threat scenario. Do not forget to cite data supporting your likelihood estimates.

7 Risk Evaluation and Prioritisation

Using the outputs from your TVA matrix and risk matrix, rank the risks, note which are acceptable, and justify your acceptance criteria. Indicate which risks require further evaluation or treatment. A table may be used for clarity.

8 Risk Treatment Planning

For each unacceptable risk, select a treatment option (avoid, mitigate, transfer or accept) and propose controls. Explain why each control is appropriate for the business. Conclude with a risk–treatment diagram linking risks to the controls you propose.

9 Conclusions and Recommendations

Summarise the most significant risks and treatments. Highlight quick wins (such as enabling port-out locks or using app-based MFA) and long-term improvements (such as adopting hardware security keys and segmenting networks). Ensure your recommendations align with the business's objectives and the regulatory environment.

References

List all of your sources in APA 7th edition format. Remember that the reference list is not included in the word count, but all intext citations are counted.

- Australian Communications and Media Authority (ACMA). *Combating phone scams.* Retrieved from `https://www.acma.gov.au/`
- Cybersecurity and Infrastructure Security Agency (CISA). *Mobile communications best practice guidance.* Retrieved from `https://www.cisa.gov/`
-
-

Add further academic articles, industry reports and news articles as appropriate.