Introduction

If you feel that any of the problems require information that you do not find in the text, then you should

- Document the necessary assumptions
- Explain why you need them

Your answers should be brief and to the point.

You need to put all your answers in a .pdf file and upload the .pdf file to Inspera before the examination time expires.

Problem 1 – (30 points in total)

You now work as the security analyzer of **one** of the following web/mobile applications.

- Vipps (mobile app)
- Uber (mobile app)
- Amazon.com (web app)
- Booking.com (web app)

Your task is to choose **one** of the above applications and make a risk-based assessment based on the RMF (Risk Management Framework).

Your tasks include:

- Task 1: Identify a minimum of 5 business goals, a minimum of 5 business assets, and a minimum of 5 business risks (5 points).

- Task 2: Identify technical risks related to the application using misuse cases and attack trees (You need to draw at least two misuse cases, three attack trees, and identify at least ten technical risks from the misuse cases and attack trees.)
    - Misuse cases and attack trees (5 points)
    - Technical risks with link to business risks (10 points)

Note: We prefer misuse cases and attack trees in graphs. You can use whatever tools to draw them. Manual drafting is also acceptable if the information on the graph is clear and precise.

Note: You shall show that the technical risks are derived from misuse case and attack tree analysis. Otherwise, points will be deducted.

Note: You need to explain the link between technical risks and business risks. Without a proper link between technical risks and business risks, points will be deduced.

Note: You do NOT need to prioritize business and technical risks.

- Task 3: Derive security requirements from each technical risk identified, and design and describe black-box penetration test cases (including test steps and expected results of each step) to verify each derived security requirement (10 points)

Note: For each listed technical risk, one corresponding security requirement and at least one test case must be listed. The test case must have test steps and expected results of each step.

To present your answers in a structured manner, you may format your solutions like:
Task 1: ...
Task 2: ...
Task 3: ...