3 b Revised) Risk modeling

I: Forget about the emergency situations. Assume instead that you are invited to become a member of a community. Hence, with respect to Figure 1, assume you are *u2* or *u3*. Assume you are invited by *u1* and are concerned that you may be victim of a scam.
Describe at least

(A) one asset,
(B) one deliberate threat,
(C) two threat scenarios,
(D) two vulnerabilities,
(E) two unwanted incidents

with respect to this situation on behalf of yourself.

II: Conduct a security risk analysis in CORAS on behalf of yourself.
You should use the seven steps of the BT Technology Journal article as a basis for the risk analysis. These steps describe the procedure for a full security analysis using the CORAS method. For this exercise you only need to use a subset of the full method. The diagrams should be prepared in the CORAS editor. Your answer should include the following:

Steps 1 to 3 – identify target of analysis etc.

- Define the target of analysis. By target of analysis we mean the parts of the system that are included in the analysis.
  Motivate the definition. Note that it may be necessary to add system aspects that are not described in the exam paper.
- Describe the focus of the analysis. By focus we mean the main concerns of the client (which in this case is yourself), what do you want to protect and what are you worried about?
- Describe the assets and document these in an asset diagram (at least three assets)
- Define a consequence scale for the identified assets
- Define a likelihood scale
- Define risk evaluation criteria for each asset by means of risk evaluation matrixes. The matrixes should have two criteria:
  a) Acceptable
  b) Unacceptable

Step 4 – risk identification

- Identify unwanted incidents towards the identified assets (at least three for each asset)
- What or who are the threats?
- Consider how these threats can initiate threat scenarios leading to the unwanted incidents. Document your findings in CORAS threat diagrams.

Step 5 – risk estimation

- Do the following for at least one path in a threat diagram:
  - Assign a frequency value to the initiate relation and probability values to the leads-to relations. Use these to compute the likelihood of the unwanted incident and document it in the threat diagram.

- Assign likelihood values to the remaining unwanted incidents and document them in the threat diagram(s).
- Assign consequence values to the unwanted incidents with regard to the affected assets and document them in the threat diagram(s).
- Answer the following:
  How many risks do the unwanted incidents in your diagrams give rise to?

Step 6 – risk evaluation

- Place the risks obtained from step 5 in the risk evaluation matrix/ices.

Step 7 – risk treatment

- Identify treatments for the unacceptable risks (if any) and document these in treatment diagrams.