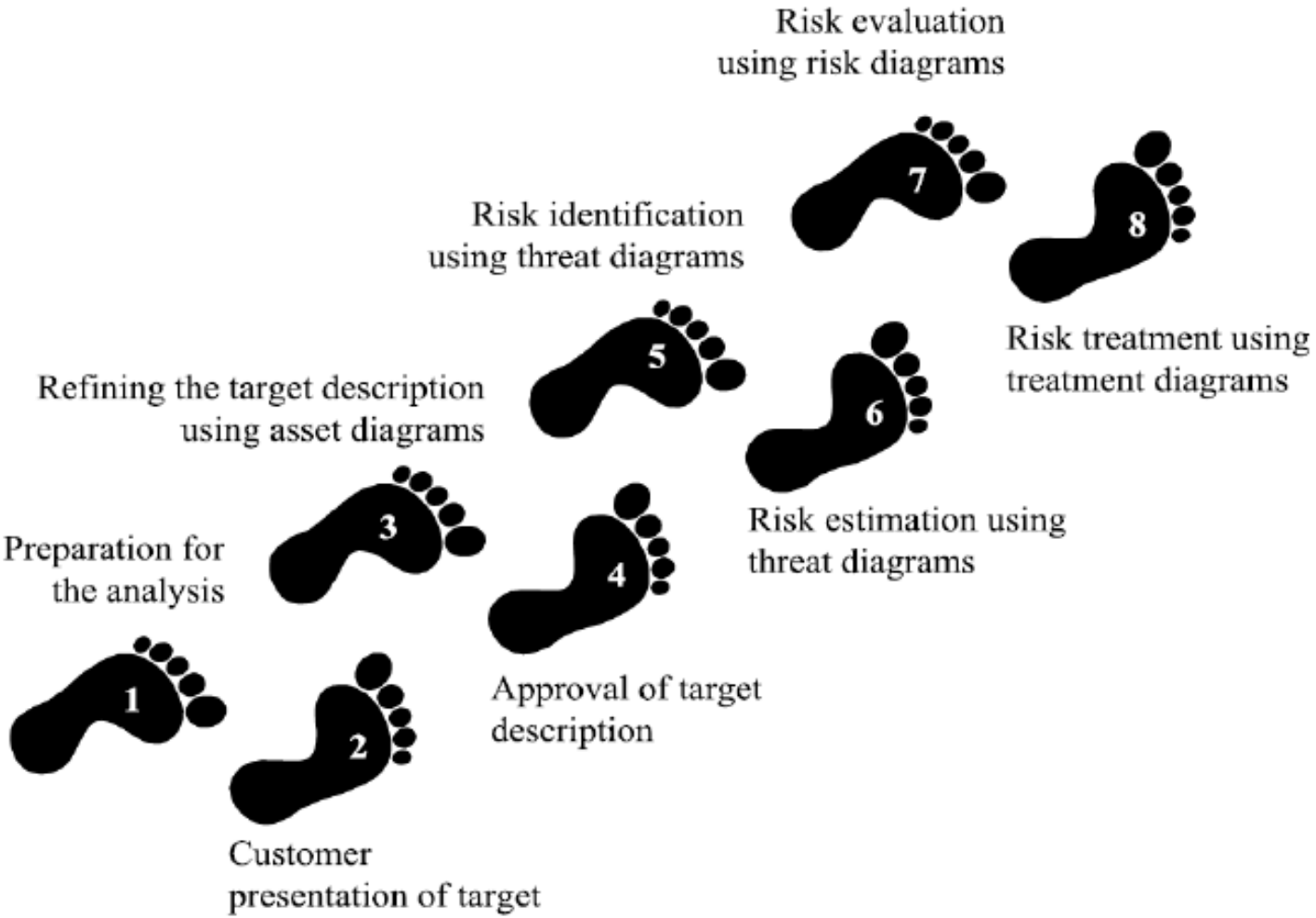
CORAS Risk Analysis Exercise

Fabio Massacci

What are we going to do

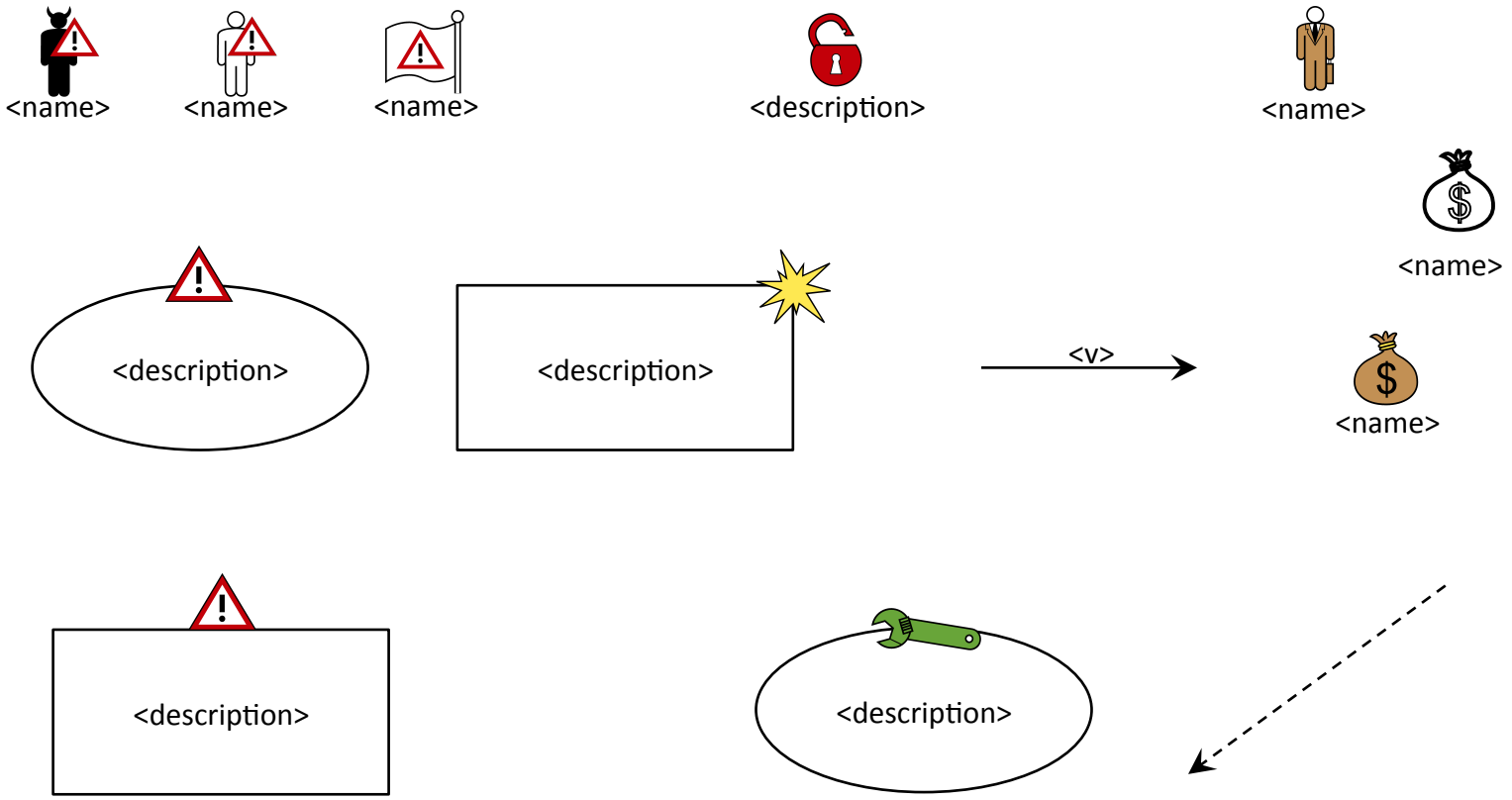
- Go to Dropbox folder
  - –Link is available on the course web page
  - –Download the file HouseRentalCase.pdf
  - –Download CORAS-exercise-template.pptx
- Read the file HouseRentalCase.pdf (10 min)
- We go through all the steps of CORAS
- Execute the step (20 min)
- Discuss the results (15-20 min)

The eight steps of a CORAS risk analysis



CORAS Palette

- Make the CORAS diagrams in the PPT slides by copy-and-paste from this palette



Step 1: Preparation for the analysis

- Objective: do the necessary initial preparations prior to the actual startup of the analysis
- Tasks:
  - Contact the customer for the case study
  - Roughly setting the scope and focus

Step 2: Customer presentation of the target

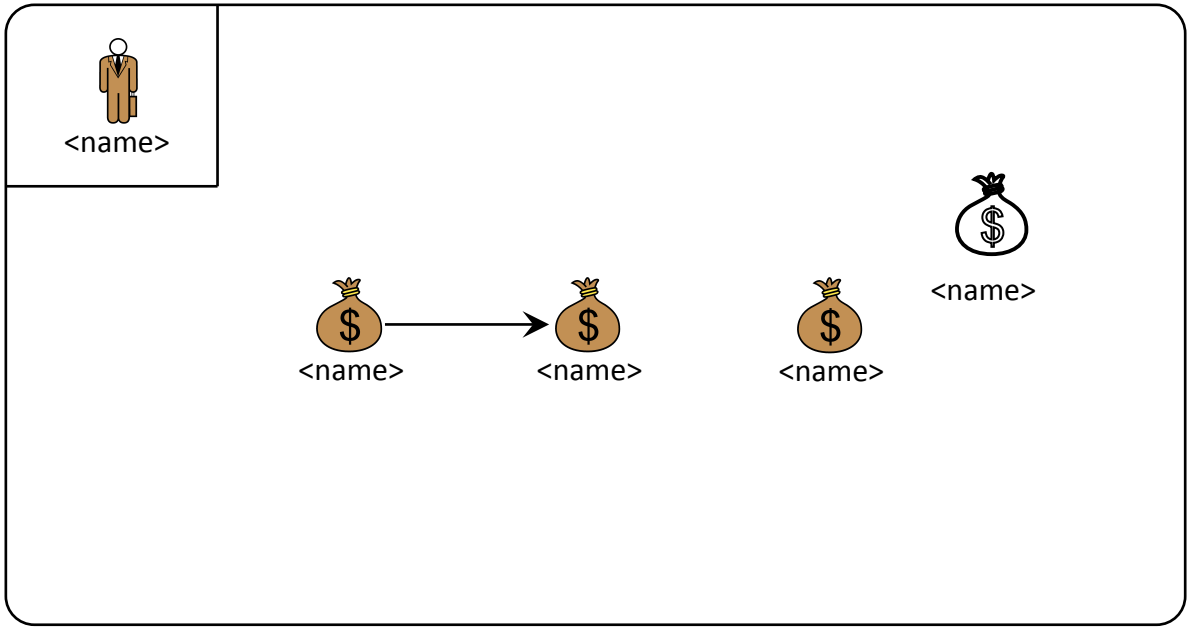
- Objective: achieve an initial understanding of the target of risk analysis
- Tasks:
  - Customer presentation on the target
  - Target to be understood by risk analysts
  - Set the focus of the analysis
- On the following blank slides you should add:
  - Description of the target:
    - The overall goals of the analysis
    - The target that wishes to have analyzed

Target of the Analysis

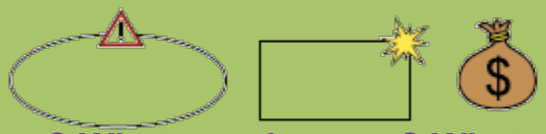
Step 3: Refining the target description using asset diagrams

- Objective: ensure a common and more precise understanding of the target analysis, including its scope, focus, and main assets
- Task:
  - The target is understood by the risk analysts
  - Identify the parties and assets
  - Conduct a high-level analysis:
    - The first threats, vulnerabilities, threat scenarios and unwanted incidents are identified.
- On the following blank slides you should add:
  - **Asset diagram**
  - High-level analysis: preliminary list of Unwanted incidents

Asset Diagram



High Level Analysis

 Who/ What is the cause?	 How? What may happen? What does it harm?	 What makes this possible?
…	…	…..
….	….	…..

Step 4: Approval of the target description

- Objective: decide a ranking of the assets; establish scales for estimating risks and criteria for evaluate risks
- Tasks:
  - Define:
    - Likelihood scale and its description
    - Consequence scale for each direct asset
  - Risk function is determined
  - Agree on Risk evaluation criteria
- On the following blank slides you should add:
  - Likelihood and Consequence scales
  - Risk function
  - Risk evaluation criteria

Likelihood and Consequence Scale

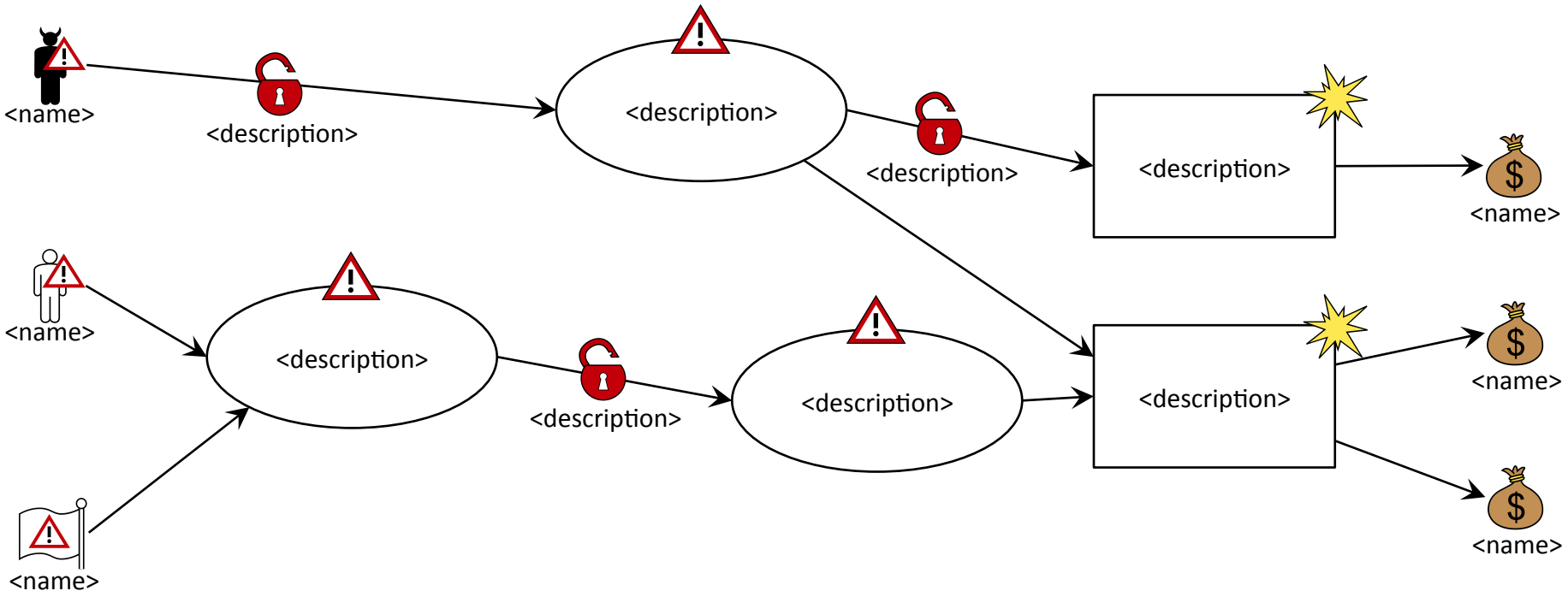
Risk Function and Evaluation Criteria

Step 5: Risk Identification using Threat diagrams

- Objective: Identify and document risks through the identification and documentation of unwanted incidents, threats, threat scenarios and vulnerabilities
- Tasks:
  - Identify risk that might harm clients' assets
    - How a **threat** exploits a **vulnerability** to cause an **unwanted incident** that harms the client's **asset**
    - *(proposed)* Sub steps*:*
      - Identify Assets and Threats
      - Identify Unwanted Incidents
      - Identify Threat Scenarios
      - Identify Vulnerabilities
- On the following blank slides you should add:
  - **Threat diagram**

Threat Diagrams

- Create your threat diagrams in the following slides, one diagram per slide
  - Each diagram should be about one "topic" or "issue"
  - For example, one diagram can address e.g. one asset, one particular kind of threat, one particular part of the target, etc.
- Complete first the risk identification, i.e. create all diagrams without considering likelihoods and consequences
- Once the risk identification is completed, use the diagrams to proceed with the risk analysis
- The next slide gives a skeleton that can be used as a starting point

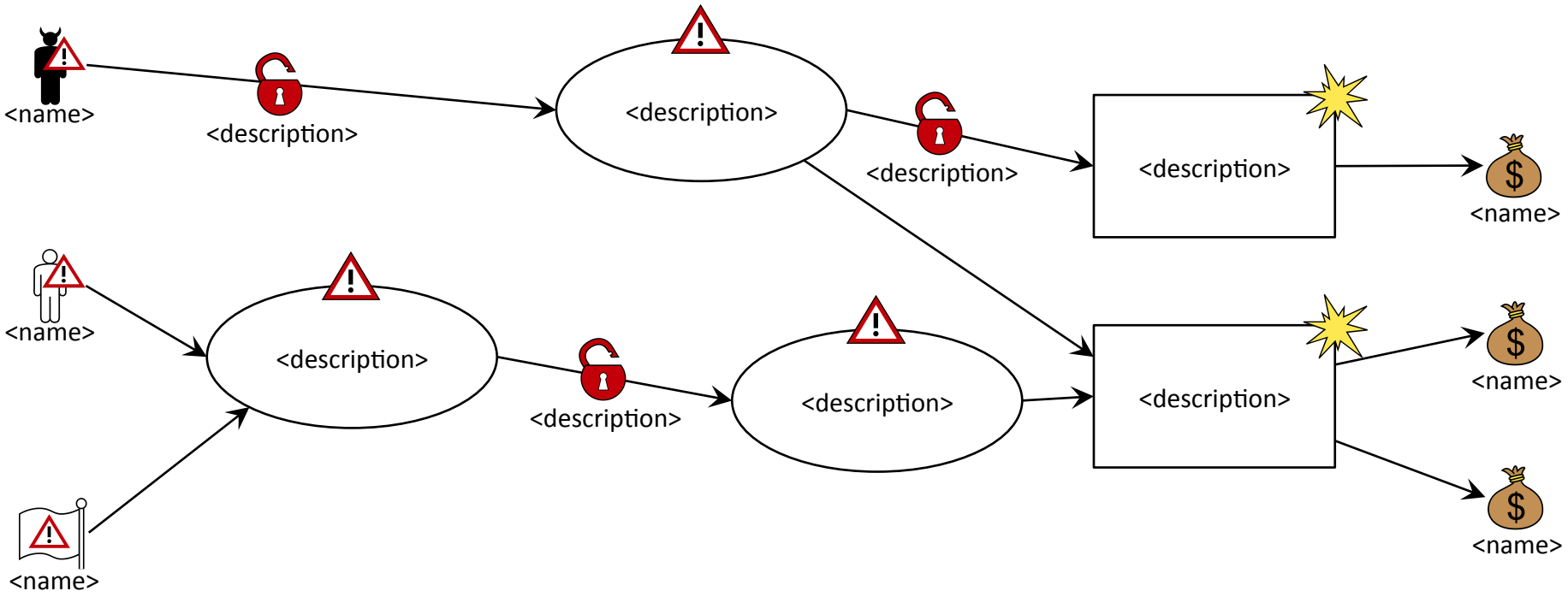

<name>
<description>
<description>
<description>
<description>
<description>
<name>
<name>
<description>
<description>
<description>
<description>
<name>
<name>
<name>

Step 6: Risk estimation using threat diagrams

- Objective: determine risk level of the identified risks
- Tasks: base on likelihood and consequence scale approved in Step 4
  - Assign likelihood estimated for each Threat Scenario
  - Assign likelihood estimated for each Unwanted Incidents
  - Assign consequence caused by each Unwanted Incidents on each Asset (the consequence is denoted on “impact” relation
- On the following blank slides you should add:
  - Completed **Threat diagrams** with likelihood and consequences assigned

Threat Diagrams

- Create your Threat diagrams in the following slides
- Copy-and-past the threat diagrams from step 5 and document likelihood and consequences by annotating these diagrams


<name>
<description>
<description>
<description>
<description>
<description>
<name>
<name>
<description>
<description>
<description>
<description>
<name>
<name>
<name>

Step 7: Risk evaluation using Risk diagram

- Objective: decide which of the identified risks are acceptable and which must be further evaluated for possible treatment
- Tasks:
  - Evaluate the identified risks:
    - Enter the risks into the **Risk Function** (from step 4)
    - Evaluate which risks are acceptable and which are not
  - Summarize the risk picture by Risk Diagram
- On the following blank slides you should add:
  - Completed **Risk Function**
  - **Risk Diagram** with evaluation result

Risk Function

Risk Diagram

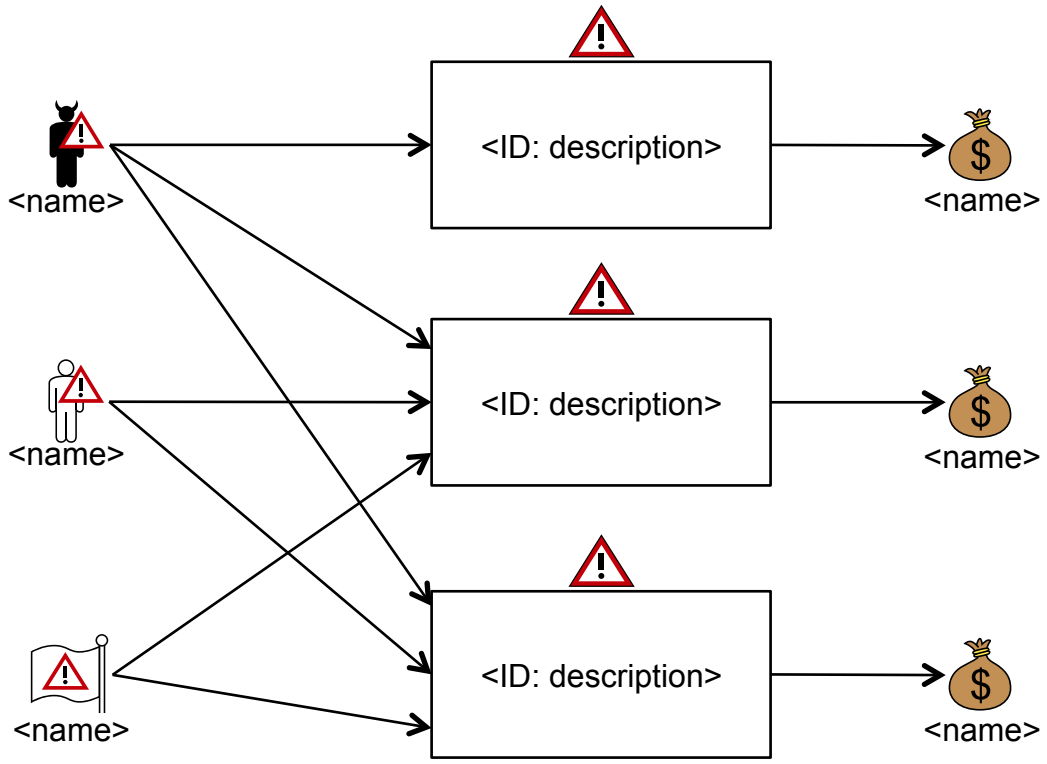


Table Summary of Risk Assessment

Asset	Risk	Likelihood	Consequence	Risk level

Step 8: Risk treatment using Treatment diagram

- Objective: identify cost effective treatments for the unacceptable risks
- Task:
  - Identify Treatment Scenario for unacceptable risks:
    - What can we do to reduce the risks to an acceptable (or monitor) level?
  - Create **Treatment diagram**
  - Summarize by **Treatment Overview diagram**
  - Evaluate treatment: estimate the cost-benefit of each treatment, and decide which ones to implement
  - Summarize the risks and treatments by filling in the **overall summary table**

- On the following blank slides you should add:
  - **Treatment diagram** (=Threat diagram with Treatment added)
  - **Treatment Overview diagram**
  - Treatment evaluation
  - Overall summary table

Treatment Diagrams

- Create your treatment diagrams in the following slides
  - How: Copy-and-past the threat diagrams from step 6 and document treatments by annotating these diagrams
- Create your treatment overview diagrams in the following slides
  - How: Copy-and-past the risk diagrams from step 7 and document treatments by annotating these diagrams

Treatment Diagrams

Treatment Overview Diagrams

Treatment Evaluation

Treatment	Cost	Risk	Risk reduction	Select to implement

Overall Summary

- Download the file CORAS-Summary of Results.xlsx.
- Fill it in and Upload it through the form
- Link to the form is available on the course web page