OBLIG III: SECURITY RISK ASSESSMENT

Please note that the oblig should be solved by each student individually. Please send your solution as an attachment by email to kst@sintef.no. The format of the solution should be pdf. The solution should be named with your name.

Since this has been missunderstood before: Your name is not your ifi-username but your official name. A named solution is not a pdf file with your name in the file name.

Security risk assessment of recruitement system

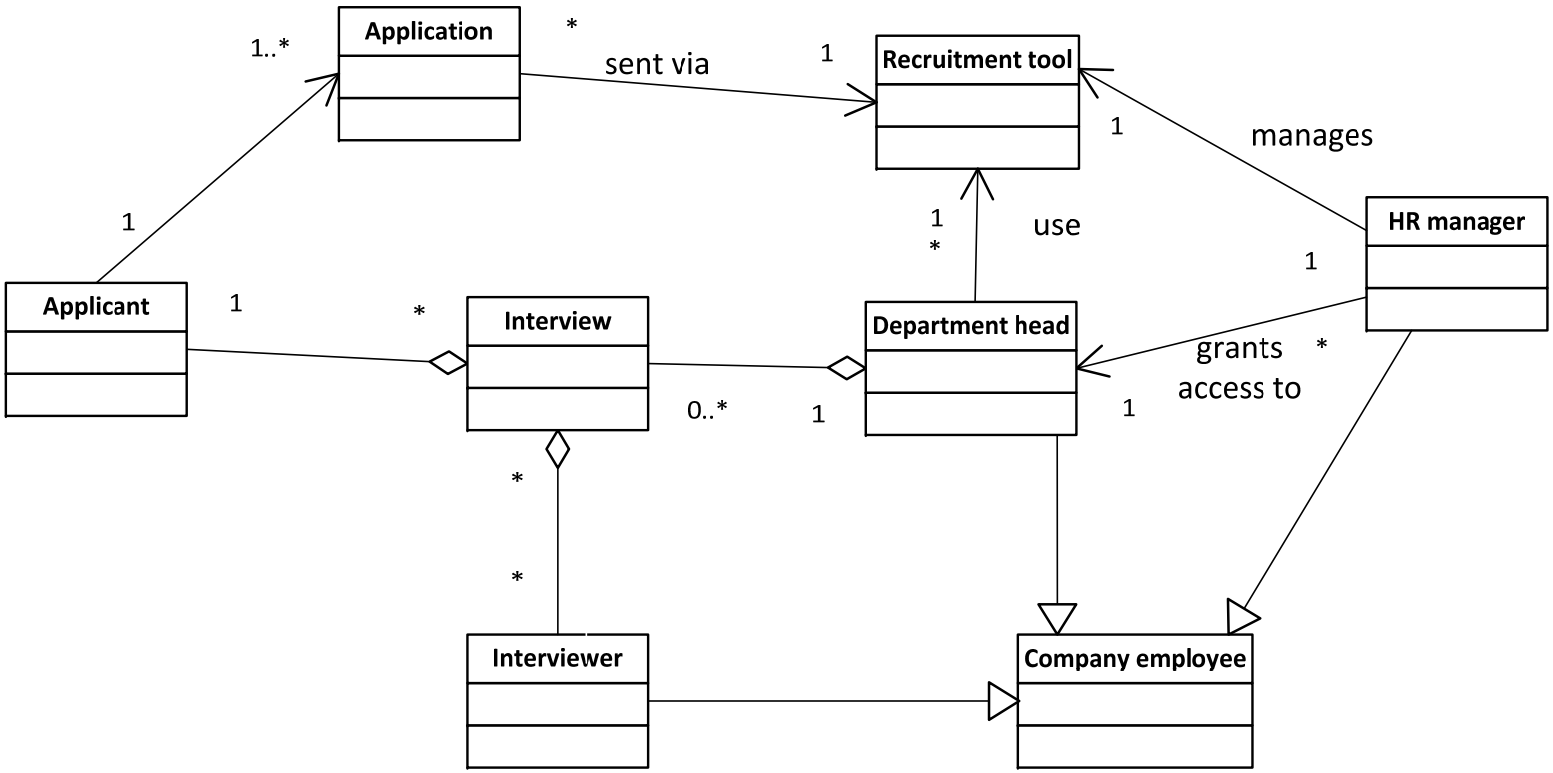
Consider again the recruitment system that you know from Oblig-I and Oblig-II.

We base ourselves on the version specified by the UML diagrams on the following three slides.

Most of the tasks you are asked to do are specified in detail in the CORAS-book and/or the cyber-risk book, both which may be downloaded freely when you are logged-in at UiO. If you have trouble downloading ask the library for help.

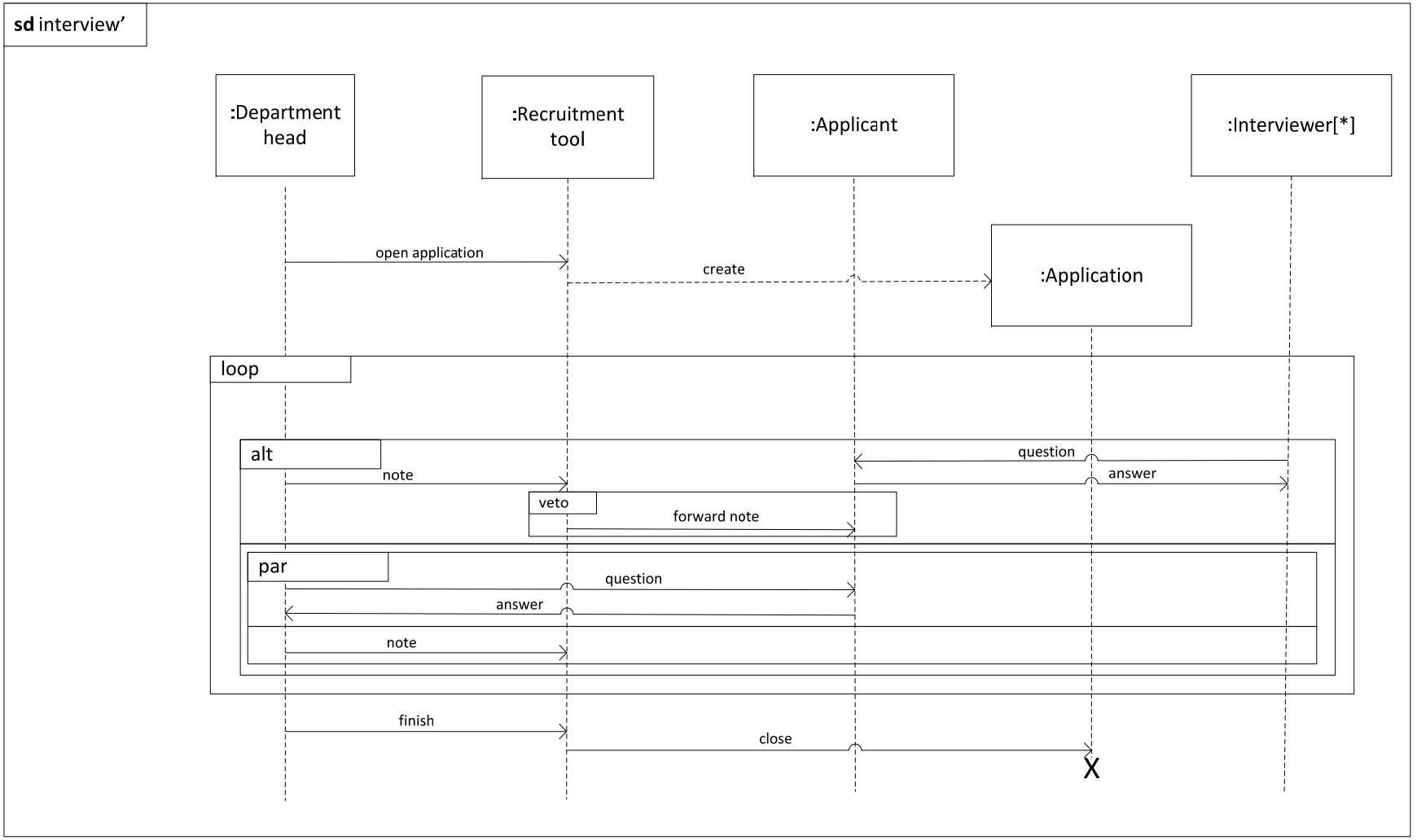
We will give more detailed references to what to read for each task.

UML Class diagram



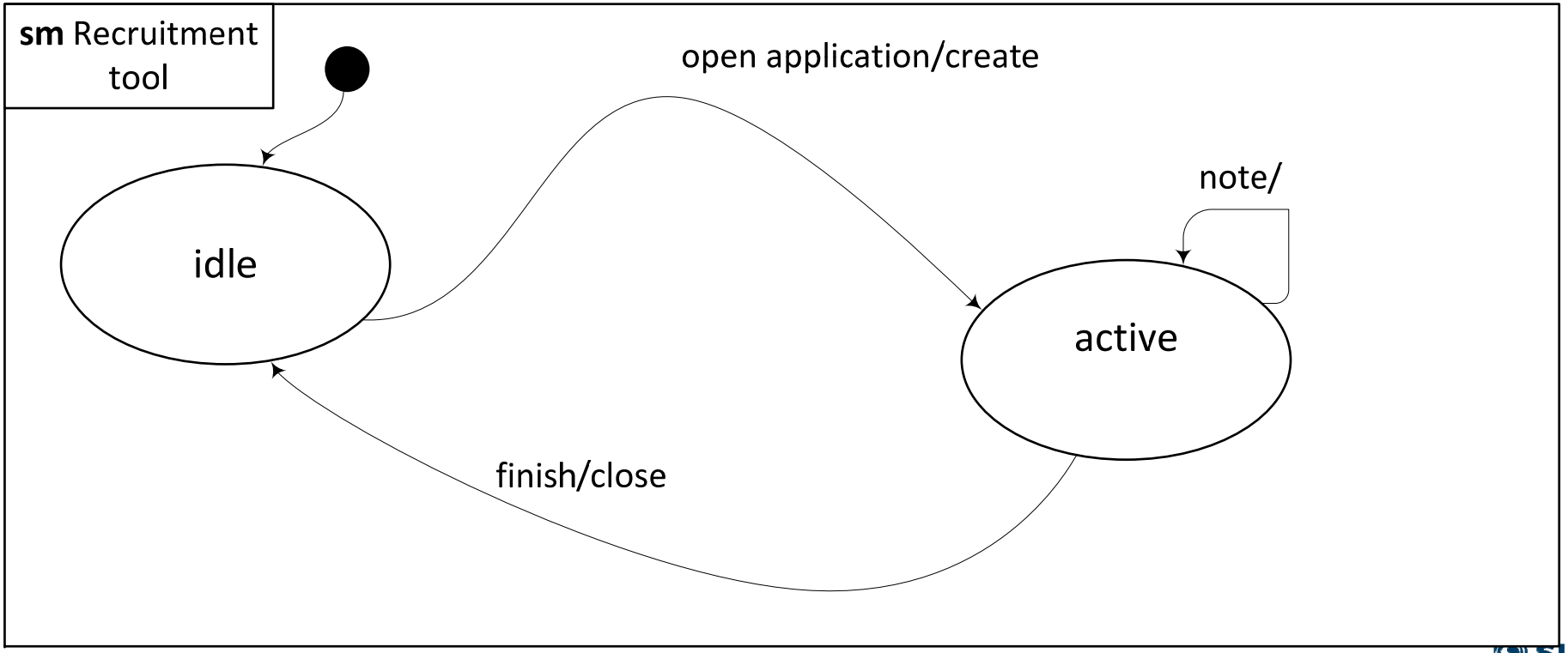
SINTEF

UML Sequence diagram



SINTEF

UML state-machine



SINTEF

Guided tour of CORAS

- To get an overview of the whole issue I strongly recommend you start by reading

  - Chapter 3: A Guided Tour of the CORAS Method

Your task

- You are to carry out various steps of a risk assessment of the recruitement system on behalf of the Bang! Company

- You may use the CORAS-tool or make use of the CORAS stencile in combination with for exampel Visio
  - See http://coras.sourceforge.net/downloads.html for both

Exercise I: Asset identification

- The customer, the company Bang!, identifies seven assets, namely compliance, integrity, reputation, database, availability, competence and privacy.
- Make a CORAS asset diagram specifying these seven assets and their relationships to the extent there are any (see Section 7.2.2 of the CORAS book).
  - Four assets should be direct including availability and privacy
  - Three assets should be indirect including reputation

Exercise II: High-level analysis

- Conduct a high-level analysis of the recruitment system with respect to the identified assets. See Section 7.2.2 of the CORAS book.

Exercise III: Define consequence scales

- Define qualitative consequence scales for the assets competence and reputation
- Define quantitative consequence scales for the assets availability and privacy
- Each scale should distinguish between 6 values

- See Section 8.2.3 of the CORAS book
- See Chapter 12 of the Cyber-Risk Management book

Exercise V: Define likelihood scale

- Define a quantitative scale for likelihoods based on 6 intervals
- The scale should use frequencies and not probabilities

- See Section 8.2.4 of the CORAS book.
- See Chapter 12 of the Cyber-Risk Management book.

Exercise IV: Define risk matrix

- We assume for simplicity that we use the same risk matrix for all assets
- Define a risk matrix (function) with 6*6 risk values and 3 risk levels

- See Sections 8.2.5 and 8.2.6 of the CORAS book

Exercise VI: Threat modelling

- Specify threat scenarios with respect to the direct assets availability and privacy using CORAS threat diagrams
- The diagrams should capture at least 7 risks and contain examples of malicious threats, non-malicious threats as well as non-human threats
- The diagrams should document relevant vulnerabilities and threat scenarios
- See Chapter 9 of the CORAS book

Exercise VII: Risk estimation

- Decorate the threat diagrams from Exercise VI with consequences and frequencies based on the scales you have defined.
- All relations between threat scenarios, unwanted incidents and combinations between these two should be assigned a conditional probability different from 1.
- Argue that the resulting diagrams are consistent.
- See Chapter 10 of the CORAS book.

Exercise VIII: Risk evaluation

- Based on the risks for the direct assets availability and privacy, estimate risks for the indirect asset reputation. (See Section 11.2.5 of the CORAS book)
- Plot the identified risks for the assets availability, privacy and reputation into the specified risk matrix. (See Section 11.2.6 of the CORAS book)

Exercise IX: Risk treatment

- Decorate the threat diagrams with treatments to reduce the risk values. (See Section 12.2.2 of the CORAS book)
- Will your proposed treatments introduce new security risks? Explain.

Deadline: November 13