Correctness and completeness will be the two major criteria to assess your solutions.

<table>
<thead>
<tr>
<th>Task</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>12</td>
</tr>
<tr>
<td>Task 2</td>
<td>16</td>
</tr>
<tr>
<td>Task 3</td>
<td>22</td>
</tr>
<tr>
<td>Task 4</td>
<td>10</td>
</tr>
<tr>
<td>Task 5</td>
<td>20</td>
</tr>
<tr>
<td>Task 6</td>
<td>15</td>
</tr>
<tr>
<td>Task 7</td>
<td>10</td>
</tr>
<tr>
<td>Test</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>135</strong></td>
</tr>
<tr>
<td><strong>Course grade</strong></td>
<td><strong>45</strong></td>
</tr>
</tbody>
</table>
Task 1: Analyse the model given in Fig. 1. Write (potentially with some explanation) one example of each function for information processing. To support your answer, fill Table 1.

<table>
<thead>
<tr>
<th>Information processing function</th>
<th>Example (and explanation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture information</td>
<td></td>
</tr>
<tr>
<td>Transmit information</td>
<td></td>
</tr>
<tr>
<td>Store information</td>
<td></td>
</tr>
<tr>
<td>Retrieve information</td>
<td></td>
</tr>
<tr>
<td>Manipulate information</td>
<td></td>
</tr>
<tr>
<td>Display information</td>
<td></td>
</tr>
</tbody>
</table>
Fig. 1: Asset modelling using misuse cases
Task 2: These security requirements are extracted from solutions of your colleagues. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.

**SecReq.1:** The football federation employee, Bob, may remove the league secretary at any time and it should be available.

**SecReq.2:** User must be logged in and have a role of “League Secretary” to confirm game report and “Team Representative” must have submitted Game Report.

**SecReq.3:** Football Federation Employee (legal secretary) needs authorization to insert the initial data, Final confirmation in the game report.

**SecReq.4:** Confirmation of game results by the team shall be allowed only for team representative and umpire who represents team and federation under action.

**SecReq.5:** Cash register computer must compare data about company car / employee ID to ERP and give warning if there is a mismatch is not explicitly defined.

**SecReq.6:** IT department must follow security advisories and patch the vulnerable systems, given that solutions are available.

**SecReq.7:** IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

**SecReq.8:** The firewall should continuously monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.
Task 3: From the security risk-aware Secure Tropos model, given in Figs. 2-5 extract information and fill in Table 2 regarding one security risk (its related assets and security countermeasures)

Table 2:

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Asset, risk, and risk treatment definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business asset</td>
<td></td>
</tr>
<tr>
<td>System asset</td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
</tr>
<tr>
<td>Threat agent</td>
<td></td>
</tr>
<tr>
<td>Attack method</td>
<td></td>
</tr>
<tr>
<td>Risk treatment decision</td>
<td></td>
</tr>
<tr>
<td>Security requirement</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
</tr>
</tbody>
</table>
Fig. 2. Security risk-aware Secure Tropos – diagram 1

Fig. 3. Security risk-aware Secure Tropos – diagram 2
Task 4: Represent security risk from Fig. 3 and Fig. 4 in **one** of these languages:

- Security risk-oriented BPMN;
- Security risk-oriented misuse cases;
- Mal-activities for security risk management.
**Task 5:** Table 3 presents some metrics gathered regarding risks 1, 2, 3, and 8. Complete Table 3 with the missing metrics (and their calculations). Use the given graphs and fill in Table 4.

Which risks are of the highest priority (highest severity)?

Write your answer to this question here:
<table>
<thead>
<tr>
<th>RiskID</th>
<th>Business asset value</th>
<th>Security objective</th>
<th>Before treatment</th>
<th>After treatment</th>
<th>Risk reduction level</th>
<th>Cost of countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Security criteria</td>
<td>Vulnerability level</td>
<td>Treat likelihood</td>
<td>Event potentiality</td>
<td>Impact level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security need</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk1</td>
<td>1</td>
<td>C=2 A=1</td>
<td>2 3 3</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk2</td>
<td>2</td>
<td>C=1 A=2</td>
<td>2 2 2</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk3</td>
<td>3</td>
<td>C=2 A=3</td>
<td>3 5 4</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk8</td>
<td>3</td>
<td>C=2 A=1</td>
<td>3 2 4 3</td>
<td>2 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4:

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Value/RRL</th>
<th>Cost/RRL</th>
<th>Value/Cost</th>
<th>Total</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9
Task 6: From business process diagram (see Fig. 6 a)

1.1: Extract security model (for the Team business asset) regarding the SRP1 pattern (Secure data from unauthorized access). Security model should be presented using SecureUML modelling language
1.2: Derive security requirements (at least 3)
Exercise 7: How security model created in Exercise 6 should be presented using UMLsec modelling language. Correctness and completeness of the model will be assessed.
Multiple choice test

Question will be answered correctly if all correct answers are selected.

1. How are components or parts of the information system that has value to the organisation and is necessary for achieving its objectives and supporting business assets, called?
   - System assets
   - Business assets
   - Security requirements
   - Controls
   - There is no correct answer

2. What is a condition over the phenomena of the environment that we wish to make true by installing the system, in order to mitigate risks?
   - Control
   - Attack method
   - System asset
   - Security requirement
   - There is no correct answer

3. What is a designed means to improve security?
   - Security requirement
   - Security criterion
   - Protected asset
   - Control
   - There is no correct answer

4. What is a potential attack, carried out by an agent that targets one or more system assets and exploits vulnerabilities of these assets?
   - Attack method
   - Threat
   - Event
   - Risk
   - There is no correct answer

5. What is a combination of a threat and one or more vulnerabilities?
   - Risk
   - Impact
   - Event
   - Threat
   - There is no correct answer

6. How are threats related to configuration and administration of the security system called?
   - Cryptography threats
   - Countermeasure design threats
   - Configuration/administration threats
   - Network protocol threats
   - There is no correct answer
7. How are threats that specifically target the network protocols used for communication called?

☐ Communication attacks
☐ Countermeasure design threats
☐ Network protocol attacks
☐ Remote information inference
☐ There is no correct answer

8. How are threats to the way certain countermeasures are (or may be) designed?

☐ Cryptography attacks
☐ Identity attacks
☐ Network protocol attacks
☐ Remote information inference
☐ There is no correct answer

9. Which security requirements describe the extent to which a system shall enable security personnel to audit the status and use of its security mechanisms?

☐ Authorisation requirements
☐ Authentication requirements
☐ Audit requirements
☐ Privacy requirements
☐ There is no correct answer

10. Which security requirements describe the extent to which a system shall survive the intentional loss or destruction of its components?

☐ Authorisation requirements
☐ Authentication requirements
☐ Audit requirements
☐ Privacy requirements
☐ There is no correct answer

11. Which security requirements describe the extent to which a system shall protect itself from physical assault?

☐ System maintenance security requirements
☐ Survivability requirements
☐ Security auditing requirements
☐ Non-repudiation requirements
☐ There is no correct answer

12. How modelling can guide elicitation of (security) requirements?

☐ Explain how security countermeasures can be captured through organisational goals
☐ It can help to figure out what questions to ask
☐ It can help to surface the hidden (security) requirements
☐ Animate the model to help visualise/validate the requirements
☐ There is no correct answer
13. Which of the following constructs are used to represent system asset in BPMN?

☐ Integrity  
☐ Lock  
☐ Misuser  
☐ Data Object  
☐ There is no correct answer

14. Which constructs are used to represent event in BPMN?

☐ Gateway  
☐ Annotation  
☐ Pool  
☐ Task  
☐ There is no correct answer

15. Which construct is used to represent targets relationship in Secure TROPOS?

☐ Means-ends  
☐ Contribution  
☐ Restricts  
☐ Attacks  
☐ There is no correct answer

16. Which of the following constructs can be used to represent security criterion in Secure TROPOS?

☐ Plan  
☐ Softgoal  
☐ Security Constraint  
☐ Hardgoal  
☐ There is no correct answer

17. Which of the following constructs can be used to represent business assets in Security risk-oriented misuse cases?

☐ Security Use Case  
☐ Secure System Agents  
☐ Misuse Case  
☐ Constraint-of Relationship  
☐ There is no correct answer

18. Which of the following constructs can be used to represent attack method in Security risk-oriented misuse cases?

☐ Misuser  
☐ Misuse case  
☐ Vulnerability  
☐ Impact  
☐ There is no correct answer
19. Which of the following constructs can be used to represent control using Mal-activities for the risk management?

- Mitigation Activity
- Malicious Activity
- Activity
- Decision
- There is no correct answer

20. Which of the following constructs can be used to represent components of event using Mal-activities for risk management?

- Mal-swimlane
- Informal comment
- Malicious Activity
- Mal-decision
- There is no correct answer

21. What does it mean when an attacker cannot sufficiently distinguish whether an item of interest (from the attacker’s perspective) exists or not?

- Anonymity
- Unlinkability
- Undetectability
- Unobservability
- There is no correct answer

22. How is this called when pseudonyms are used as identifiers?

- Anonymity
- Identiability
- Unobservability
- Pseudonymity
- There is no correct answer

23. How is the process of limiting access to the resources of a system only to authorised programs, processes or other systems called?

- Access
- Access control
- Permission assignment
- Session
- There is no correct answer

24. How is a passive entity that contains or receives information called?

- Administrator
- Object
- Subject
- Session
- There is no correct answer
25. What are patterns for operating system access control about?

☐ Full access with errors
☐ Limited access
☐ Access control in operating systems
☐ Malicious activity access
☐ There is no correct answer

26. What are patterns for access control models?

☐ Role-based access control model
☐ Malicious activity models
☐ Authorisation model
☐ Multilevel model
☐ There is no correct answer

27. System access control architecture patterns describes essentials for system that permit or deny their use explicitly. These patterns deal with the architecture of the software systems. What are their types:

☐ Security sessions
☐ Limited access
☐ Single point access
☐ Communication access limits
☐ There is no correct answer

28. Which steps do not belong to the security requirements elicitation from business processes (the SREBP method)?

☐ Identify business assets
☐ Analyse and assess security risks
☐ Determine security objectives
☐ Identify patterns, extract security model and derive security requirements
☐ There is no correct answer

29. What components needs to be identified when securing data transmitted between business entities?

☐ Functional-unit and business partner
☐ Input interface and input data
☐ Secret key and private key
☐ Communicators and data transmission
☐ There is no correct answer

30. What are the seven security touchpoints?

☐ Code review
☐ Risk analysis and sisk based security testing
☐ Security requirement and penetration testing
☐ Abuse analysis and security requirements
☐ There is no correct answer