Evaluation results

<table>
<thead>
<tr>
<th>Test, exercises</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test II</td>
<td>/ 10</td>
</tr>
<tr>
<td>Exercise 1:</td>
<td>/ 8</td>
</tr>
<tr>
<td>Exercise 2:</td>
<td>/ 8</td>
</tr>
<tr>
<td>Exercise 3:</td>
<td>/ 4</td>
</tr>
<tr>
<td>TOTAL:</td>
<td>/ 30</td>
</tr>
<tr>
<td>(            / 5 course points)</td>
<td></td>
</tr>
</tbody>
</table>

Test II

1. Which constructs are used to represent threat agent in BPMN?  
   □ Task  
   □ Lane  
   □ Pool  
   □ Event  
   1 point

2. Which constructs are used to represent business assets in BPMN?  
   □ Gateway  
   □ Data Store  
   □ Data Object  
   1 point

3. Which of the following constructs can be used to refer to vulnerability in Secure TROPOS?  
   □ Hardgoal  
   □ Vulnerability point  
   □ Plan  
   □ Resource  
   1 point

4. Which of the following constructs can be used to represent system assets in Secure TROPOS?  
   □ Hardgoal  
   □ Plan  
   □ Softgoal  
   □ Resource  
   1 point

5. Which constructs are used to represent impact in BPMN?  
   □ Annotation  
   □ Task  
   □ Lock  
   1 point
6. Which construct is used to represent threat agent in Secure TROPOS?  
☐ Plan  
☐ Resource  
☐ Actor  

7. Which of the following constructs are used to represent system asset in BPMN?  
☐ Pool  
☐ Lock  
☐ Data Object  

8. Which construct is used to represent attack method in Secure TROPOS?  
☐ Resource  
☐ Plan  
☐ Actor  

9. Which of the following constructs can be used to represent security criterion in Secure TROPOS?  
☐ Plan  
☐ Softgoal  
☐ Security Constraint  
☐ Hardgoal  

10. Which construct is used to represent vulnerability in BPMN?  
☐ Event  
☐ Task  
☐ Annotation
**Exercise 1:** Taken into account values given in the Table below, which risks\(^1\) are of the highest priority (highest severity)?

<table>
<thead>
<tr>
<th>Security Risks</th>
<th>Business asset value (acorns)</th>
<th>Risk reduction level (unit levels)</th>
<th>Cost of security countermeasure (euro)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk 1:</strong> A vandal having desire to mix the data, queries the Game storage, modifies the data files, because of incorrect use of access control leading to fixing the bug, modified game storage and not reliable data to generate game report.</td>
<td>100</td>
<td>4</td>
<td>5000</td>
</tr>
<tr>
<td><strong>Risk 2:</strong> A vandal having no experience and having a motive to intervene in the system, stoles identity of Football Federation Employee and makes false game information input, leading to false game information, not reliable data to store and negation of user identity.</td>
<td>150</td>
<td>5</td>
<td>4500</td>
</tr>
<tr>
<td><strong>Risk 3:</strong> A specialist having a motivation to examine the code of IS in order to introduce new features and security tendencies is abusing weak algorithm because of code manipulation while gaining game information and creating game record in the system, leading to poorly gathered game information, wrong game report generated and negation of system algorithm.</td>
<td>300</td>
<td>2</td>
<td>3000</td>
</tr>
<tr>
<td><strong>Risk 4:</strong> A spy with motivation to gain the information and modify game reports and game information knowing how to use system vulnerability right after the Football Federation Employee has given its confirmation of game report to intercept the communication between Football Federation Employee and ERIS, because of incorrect use of cryptography in communication, leading to modified game report, disturbed and not trustworthy information and negation of secrecy of game information and reports.</td>
<td>50</td>
<td>6</td>
<td>4500</td>
</tr>
<tr>
<td><strong>Risk 5:</strong> A trespasser with motive to brag to his fellow programming students, intercepts communication between the Football Federation Employee and ERIS, steals account information and login, because of the incorrect use of access controls in communication between ERIS and Football Federation Employee, leading to bypassed access controls and stolen Football Federation Employee’s data.</td>
<td>250</td>
<td>3</td>
<td>1500</td>
</tr>
</tbody>
</table>

---

\(^1\) These risks are extracted from the previous student solutions.
**Exercise 2:** From the security risk-aware Secure Tropos model, given in Figs. 1-5 extract information and fill in Table 1 regarding one security risk (its related assets and security countermeasures).  

8 points

<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. 1: Modelling Business Assets

Fig. 2: Security Criterion and Asset Refinement
Fig. 3: Identification of Security Risk

Fig. 4: Attack Scenario
Exercise 3: Which types of security requirements are modelled in the BPMN diagram given in Fig. 6?

4 points

- Identification requirements
- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Privacy requirements
- Non-repudiation requirements
- Security auditing requirements
- Survivability requirements
- Physical protection requirements
- System maintenance security requirements