Creativity – your key to secure software!!!
T2. What are *business assets*, *IS assets*, and what is the *support* relationship between different assets? What are *security criteria*? (8 points)

<table>
<thead>
<tr>
<th>Assets</th>
<th>Business assets</th>
<th>Information System assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support relationship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

T3. What are *risk* and its components? (7 points)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Impact</th>
<th>Event</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Threat agent</th>
<th>Attack method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**T4.** What are risk treatment decision, security requirements and potential security controls which implement suggested security requirements?  
(Hint: security requirements must satisfy criteria for good security requirements)  
(10 points)

<table>
<thead>
<tr>
<th>Risk treatment decision</th>
<th>Security requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Controls</td>
<td></td>
</tr>
</tbody>
</table>

**PART II: Security Risk Modelling**

**Introduction:** Select one graphical modelling language and create a model following your answers given for tasks T1-T4. You can choose any modelling language presented during the course or modelling language, which you experienced before.

(if you select language, which was not analysed during the course, give short introduction on language syntax and semantics)

**Selected graphical modelling language:**

Using selected modelling language you need to create three diagrams:

**T5.** Diagram for context, assets, and security criteria visualisation. Input for the diagram – your answers given for T1 and T2.  
(10 points)

**T6.** Diagram for security risk visualisation. Input for diagram is your answer given for T3.  
(10 points)

**T7.** Diagram for security countermeasure visualisation. Input for diagram is your answer for T4.  
(10 points)
**Creativity – your key to secure software!!!**

**T8.** Discuss what are benefits of security modelling when developing software systems.  

**PART III: Modelling Role-based Access Control Policy**

**Introduction:** Define the role-based access control (RBAC) policy for the given scenario (see below). When preparing the policy, answer and complete the given questions and tasks.

**T9.** What are the protected object, its attributes, and its protected operations? Please use the class diagram notation to answer this question.

**T10.** What are the roles and potential actors involved in this scenario?

<table>
<thead>
<tr>
<th>Roles</th>
<th>Actors</th>
<th>Role actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Client</td>
<td>Aleksandr Skafandr …</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creativity – your key to secure software!!!

T11. Prepare the UMLsec model (i.e., the UML activity diagram extended for the RBAC modelling) to visualise the RBAC policy for the given scenario.  
(10 points)

T12. Write down all needed authorisation constraints.  
(10 points)

Client Placing a Purchase Order Scenario

The process starts with client filling in an order form. Client specifies his contact info and requested items and sends the request to the seller. Seller views the purchase order and assigns unit codes and prices to the offering and sends the document to delivery team. Delivery department will specify when they can ship the package to the client. After the offering is complete it will be sent back to the client for acceptance. If the client refuses the offering, then the process stops and the document is deleted. If the offering is accepted by the client the document is sent to the accounting department who will transmission a credit card payment. If the payment is accepted, then accounting department will mark the order as being paid and send it to delivery department. The delivery department will pack and ship the ordered items and mark the order as shipped.

Purchase order form

<table>
<thead>
<tr>
<th>No.</th>
<th>Quantity</th>
<th>Item Code</th>
<th>Description</th>
<th>Unit Price</th>
<th>Amount</th>
<th>Delivered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100.00 PCS</td>
<td>INV00005</td>
<td>1900mAh Slim Battery Charging Case for iPhone 4/4S</td>
<td>15.00</td>
<td>1,500.00</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>200.00 PCS</td>
<td>INV00006</td>
<td>2400mAh Solar Powered Rechargeable Battery Pack for iPhone or iPad</td>
<td>12.00</td>
<td>2,400.00</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>200.00 PCS</td>
<td>INV00002</td>
<td>Apple iPad casing - black</td>
<td>20.00</td>
<td>4,000.00</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>200.00 PCS</td>
<td>INV00003</td>
<td>Samsung Galaxy Tab 10.1&quot; casing - black</td>
<td>10.00</td>
<td>2,000.00</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>200.00 PCS</td>
<td>INV00001</td>
<td>Apple iPad casing - white</td>
<td>20.00</td>
<td>4,000.00</td>
<td>X</td>
</tr>
</tbody>
</table>

Payment Info
Cardholder's name: Aleksandr Skafandr
Card Number: 21321312312312312 Exp. Date: 01-May-2015

Payment Accepted
Multiple-Choice Questionnaire
[Each correctly answered question gives 1 point]

1. What is risk mitigation?
   a) A risk treatment decision not to become involved in a risk;
   b) A risk treatment decision to share with another party the burden of loss from a risk;
   c) A risk treatment decision to accept the burden of loss from a risk;
   d) A risk treatment decision to lessen the negative consequence associated with the risk;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

2. What is security needs?
   a) A standard means by which a threat agent carries out a threat;
   b) A characteristic of business asset that constitute a weakness or a flaw in terms of security;
   c) A security objective that characterises the application of a security criterion on a business asset;
   d) A property on business asset that describes object effectiveness, availability and defensibility;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

3. What are attack trees?
   a) A way of thinking and describing security of systems and subsystems;
   b) A way of capturing security expertise and reusing it;
   c) A potential attack, carried out by an agent that may lead to harm to assets;
   d) A combination of a threat vulnerabilities and impact;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

4. To what functionality components system could be decomposed?
   a) User interactions;
   b) Data/storage and resource management;
   c) Distributed controls;
   d) Communication and addressing;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

5. What is survivability?
   a) Degree to which essential, mission-critical services continue to be neglected in spite of either accident or malicious harm;
   b) Degree to which various kinds of users can depend;
   c) A target of safety level that is expected to meet by the information system;
   d) Estimation of trustworthy characteristics of the analysed system;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.
6. What is **pretexting**?
   a) Trojan horse variant that uses physical media and relies on curiosity of victim;
   b) Action of stealthily observing the target to obtain confidential information;
   c) Act of creating and using an invented scenario to divulge target’s sensitive information;
   d) Giving something to get something in return;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

7. What is **CLASP**?
   a) Open web application security project;
   b) A device (as a hook) for holding objects or parts together;
   c) Comprehensive lightweight application security process;
   d) Cigital security touchpoints;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

8. What is **security pattern**?
   a) A particular recurring security problem;
   b) A specific security context where problems occur;
   c) A well-proven generic security scheme for a security solution;
   d) All a, b, and c;
   e) Neither a, b, c nor d.

9. What is **unlinkability**?
   a) When pseudonyms are used as identifiers;
   b) When it is not possible sufficiently distinguish whether item of interest exists or not;
   c) When it is not possible sufficiently distinguish whether these items of interest are related or not;
   d) When item of interest is not identifiable within a set of subjects;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

10. What are **intrusion detection requirements**?
   a) Requirements that characterise the extent to which a business, application, or component shall verify the identity of its externals before interacting;
   b) Requirements that characterise the extent to which an application or component shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion;
   c) Requirements that characterise the extent to which a business, application, or component shall keep its sensitive data and communications private from unauthorized individuals and programs;
   d) Requirements that characterise the extent to which an application or component shall detect and record attempted access or modification by unauthorized individuals;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.