Lecture 7

→ Requirements Prioritisation

→ Risk Management
Lecture 7

→ Requirements Prioritisation

→ Risk Management
Basics of Prioritisation

→ Need to select what to implement
  ➡ Customers (usually) ask for way too much
  ➡ Balance time-to-market with amount of functionality
  ➡ Decide which features go into the next release

→ For each requirement/feature, ask:
  ➡ How important is this to the customer?
  ➡ How much will it cost to implement?
  ➡ How risky will it be to attempt to build it?

→ Perform Triage:
  ➡ Some requirements *must* be included
  ➡ Some requirements should definitely be excluded
  ➡ That leaves a pool of “nice-to-haves”, which we must select from.
A Cost-Value Approach

→ Calculate return on investment
  ➡ Assess each requirement’s importance to the project as a whole
  ➡ Assess the relative cost of each requirement
  ➡ Compute the cost-value trade-off:
A Cost-Value Approach

→ **Calculate return on investment**
  - Assess each requirement’s importance to the project as a whole
  - Assess the relative cost of each requirement
  - Compute the cost-value trade-off:

→ **Two approaches:**
  - **Absolute scale (e.g. dollar values)**
    - Requires much domain experience
  - **Relative values (e.g. less/more; a little, somewhat, very)**
    - Much easier to elicit
    - Prioritization becomes a sorting problem
Some complications

→ Hard to *quantify* differences
  ✔ easier to say “x is more important than y”…
  ✔ …than to estimate by how much.

→ Not all requirements comparable
  ✔ E.g. different level of abstraction
  ✔ E.g. core functionality vs. customer enhancements

→ Requirements may not be independent
  ✔ No point selecting between X and Y if they are mutually dependent

→ Stakeholders may not be consistent
  ✔ E.g. If X > Y, and Y > Z, then presumably X > Z?

→ Stakeholders might not agree
  ✔ Different cost/value assessments for different types of stakeholder
Hierarchical Prioritisation

→ Group Requirements into a hierarchy
  ➔ e.g. A goal tree

→ Only make comparisons between branches of a single node:
Analytic Hierarchy Process (AHP)

Source: Adapted from Karlsson & Ryan 1997

→ Create n x n matrix (for n requirements)
  - For element (x,y) in the matrix enter:
    - 1 - if x and y are of equal value
    - 3 - if x is slightly more preferred than y
    - 5 - if x is strongly more preferred than y
    - 7 - if x is very strongly more preferred than y
    - 9 - if x is extremely more preferred than y
    - (use the intermediate values, 2, 4, 6, 8 if compromise needed)
  - ...and for (y,x) enter the reciprocal.

→ Estimate the eigenvalues:
  - E.g. “averaging over normalized columns”
    - Calculate the sum of each column
    - Divide each element in the matrix by the sum of it’s column
    - Calculate the sum of each row
    - Divide each row sum by the number of rows

→ This gives a value for each requirement:
  - ...giving the estimated percentage of total value of the project
### AHP example - estimating costs

**Req1** - 26% of the cost  
**Req2** - 50% of the cost  
**Req3** - 9% of the cost  
**Req4** - 16% of the cost

<table>
<thead>
<tr>
<th></th>
<th>Req1</th>
<th>Req2</th>
<th>Req3</th>
<th>Req4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req1</td>
<td>1</td>
<td>1/3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Req2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Req3</td>
<td>1/2</td>
<td>1/5</td>
<td>1</td>
<td>1/3</td>
</tr>
<tr>
<td>Req4</td>
<td>1/4</td>
<td>1/3</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

- Normalise columns
- Sum the rows
- Result

<table>
<thead>
<tr>
<th></th>
<th>sum</th>
<th>sum/4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req1</td>
<td>1.05</td>
<td>0.26</td>
</tr>
<tr>
<td>Req2</td>
<td>1.98</td>
<td>0.50</td>
</tr>
<tr>
<td>Req3</td>
<td>0.34</td>
<td>0.09</td>
</tr>
<tr>
<td>Req4</td>
<td>0.62</td>
<td>0.16</td>
</tr>
</tbody>
</table>
Repeat AHP process twice:
- Once to estimate relative value
- Once to estimate relative cost
Other selection criteria

Cost (percent)
Value (percent)

Above average value  
Below average cost

Above average cost  
Below average value

Relative Loss
Relative Probability

High Risk Exposure
Low Risk Exposure
Security Risk Management in Airline Turnaround Sector

→ Check-in passenger information
  - Risk1: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - Risk2: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

→ Luggage information
  - Risk3: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - Risk4: The personnel accepts luggage and adds contraband items to a passenger’s luggage

→ Fuel slip
  - Risk5: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - Risk6: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

→ Cargo assignment
  - Risk7: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - Risk8: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider

[Matulevičius et al., 2016]
FDSE 2016
Security Risk Management in Airline Turnaround Sector

Risk1: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed

Risk2: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

Risk3: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft

Risk4: The personnel accepts luggage and adds contraband items to a passenger’s luggage

Risk5: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained

Risk6: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

Fuel slip

Risk7: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider

Risk8: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider

[Matulevičius et al., 2016]
FDSE 2016
Security Risk Management in Airline Turnaround Sector

- **Check-in passenger information**
  - **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- **Luggage information**
  - **Risk3**: Personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - **Risk4**: Personnel accepts luggage and adds contraband items to a passenger’s luggage

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - **Risk6**: Attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - **Risk8**: Attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider

---

<table>
<thead>
<tr>
<th>Risk</th>
<th>Value-RRL</th>
<th>RRL-cost</th>
<th>value-cost</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Graph 1</td>
<td>Graph 2</td>
<td>Graph 3</td>
<td></td>
</tr>
<tr>
<td>Risk1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>High priority</td>
</tr>
<tr>
<td>Risk3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk4</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>High priority</td>
</tr>
<tr>
<td>Risk5</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>High priority</td>
</tr>
<tr>
<td>Risk6</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>High priority</td>
</tr>
<tr>
<td>Risk7</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Low priority</td>
</tr>
</tbody>
</table>

[Matulevičius et al., 2016]
FDSE 2016
Requirements Prioritization

→ Why Prioritization is needed
  ➸ Basic Trade-offs

→ Cost-Value Approach
  ➸ Sorting Requirements by cost/value
  ➸ Estimating Relative Costs/Values using AHP
Requirements Prioritisation

Risk Management
Risk Management

→ About Risk
  ✏️ Risk is “the possibility of suffering loss”
  ✏️ Risk itself is not bad, it is essential to progress
  ✏️ The challenge is to manage the amount of risk

→ Two Parts:
  ✏️ Risk Assessment
  ✏️ Risk Control

→ Useful concepts:
  ✏️ For each risk: Risk Exposure
    ➢ $RE = p(\text{unsat. outcome}) \times \text{loss(unsat. outcome)}$
  ✏️ For each mitigation action: Risk Reduction Leverage
    ➢ $RRL = (RE_{\text{before}} - RE_{\text{after}}) / \text{cost of intervention}$
Continuous Risk Management

→ **Identify:**
  - Search for and locate risks before they become problems
    - Systematic techniques to discover risks

→ **Analyse:**
  - Transform risk data into decision-making information
  - For each risk, evaluate:
    - Impact
    - Probability
    - Timeframe
  - Classify and Prioritise Risks

→ **Plan**
  - Choose risk mitigation actions

→ **Track**
  - Monitor risk indicators
  - Reassess risks

→ **Control**
  - Correct for deviations from the risk mitigation plans

→ **Communicate**
  - Share information on current and emerging risks

*Source: Adapted from SEI Continuous Risk Management Guidebook*
Risk Assessment

→ **Quantitative:**
  - Measure risk exposure using standard cost & probability measures
  - Note: probabilities are rarely independent

→ **Qualitative:**
  - Develop a risk classification matrix:

<table>
<thead>
<tr>
<th>Undesirable outcome</th>
<th>Likelihood of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very likely</td>
</tr>
<tr>
<td>(5) Loss of Life</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>(4) Loss of Spacecraft</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>(3) Loss of Mission</td>
<td>Severe</td>
</tr>
<tr>
<td>(2) Degraded Mission</td>
<td>High</td>
</tr>
<tr>
<td>(1) Inconvenience</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Top 10 Development Risks
(+ Countermeasures)

→ Personnel Shortfalls
  ◦ use top talent
  ◦ team building
  ◦ training

→ Unrealistic schedules/budgets
  ◦ multisource estimation
  ◦ designing to cost
  ◦ requirements scrubbing

→ Developing the wrong software functions
  ◦ better requirements analysis
  ◦ organizational/operative analysis

→ Developing the wrong User Interface
  ◦ prototypes, scenarios, task analysis

→ Gold Plating
  ◦ requirements scrubbing
  ◦ cost benefit analysis
  ◦ designing to cost

→ Continuing stream of reqts changes
  ◦ high change threshold
  ◦ information hiding
  ◦ incremental development

→ Shortfalls in externally furnished components
  ◦ early benchmarking
  ◦ inspections, compatibility analysis

→ Shortfalls in externally performed tasks
  ◦ pre-award audits
  ◦ competitive designs

→ Real-time performance shortfalls
  ◦ targeted analysis
  ◦ simulations, benchmarks, models

→ Straining computer science capabilities
  ◦ technical analysis
  ◦ checking scientific literature
Risk Management

→ **Risk Management is a systematic activity**
  - Requires both technical and management attention
  - Requires system-level view
  - Should continue throughout a project

→ **Techniques exist to identify and assess risks**
  - E.g. fault tree analysis
  - E.g. Risk assessment matrix

→ **Risk and Requirements engineering**
  - Risk analysis can uncover new requirements
    - Especially for safety-critical or security-critical applications
  - Risk analysis can uncover feasibility concerns
  - Risk analysis will assist in appropriate management action
Misuse cases

→ A modeling technique – use cases
  ➜ Normal actors and wanted functionality +
  ➜ Mis-users, harmful acts

→ Makes it possible to discuss
  ➜ Security requirements together with functional requirements.
  ➜ With a technique that is
    ➢ In normal use
    ➢ Relatively easy to understand for end-users

→ As with use-cases, there are two possibilities:
  ➜ Diagrams
  ➜ Textual descriptions
Misuse cases

- A modeling technique – use cases
  - Normal actors and wanted functionality +
  - Mis-users, harmful acts

- Makes it possible to discuss
  - Security requirements together with functional requirements.

- A
  - Diagrams
  - Textual descriptions
Security risk management process
1. Context and Assets Identification
2. Security Objectives Determination

⇒ Description of organisation and its environment
⇒ sensitive activities related to information security
3. Risk Analysis
3. Risk Analysis
4. Risk Treatment Decisions

<table>
<thead>
<tr>
<th>Risk treatment decisions</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoiding risk</td>
<td>Decision not to be involved in, or to withdraw from a risk</td>
</tr>
<tr>
<td>Transferring risk</td>
<td>Sharing with another party the burden of loss for a risk</td>
</tr>
<tr>
<td>Retaining risk</td>
<td>Accepting the burden of loss from a risk</td>
</tr>
<tr>
<td>Reducing risk</td>
<td>Action to lessen the probability, negative consequences, or both, associated with a risk</td>
</tr>
</tbody>
</table>
5. Security Requirements Definition
5. Security Requirements Definition
What have we learnt today?

→ Requirements Prioritisation

→ Risk Management