Introduction to Risk Management for Software Projects

Peter Kolb
Purpose of Presentation

- To provide an Overview of the Risk Management Process
- To describe Specific Risks with Distributed and Outsourced Software Engineering
- To explain Software Product Risk Management
Objectives of Project Risk Management

**Improve the predictability of a project!**

By:

- Raising awareness and visibility of risks
- Managing risks by mitigation actions to prevent major disasters
- Preparing for contingency
What Is A Risk?

- A Risk is a Potential Event with Negative Consequences that Has Not Happened Yet.
  - However a Risk could also be defined as the event with unforeseen positive consequences.

- A Possibility of Loss — Not the Loss Itself!
  - A source of problem during a project
  - Avoid labeling the cost of a risk as a risk (e.g. schedule slippage). Find the causes!
  - Strike at the root of the problem, not the leaves!

- Something that Makes the Project Special
  - In the widest sense everything is a risk
  - There are better ways of handling recurrent problems!
Sequence of Events

- 1. Failure, cause of hazard
Sequence of Events

2. Hazard [Gefährdung] = potential source of harm
3. Hazardous event
... which has a certain likelihood
Sequence of Events

4. Harm [Schaden, Unheil]

...which has a certain severity
Definition of Risk

Risks are defined by their

- Likelihood of Occurrence of Harm and
- Severity of Harm
Project Predictability

![Project cost graph](image)

- **Planned**
- **Not Risk Managed**

Time (months)

Cost/Planned (%)

Project cost

Project end
Project Predictability

![Project Predictability Graph]

- **Planned**
- **Risk Managed**
- **Not Risk Managed**

**Time (months)**

**Cost/Planned (%)**

- Project cost
- Project end

- Time (months)
- Project end
### Risk Management

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COTS dependency</td>
<td>Windows XP SP xy, ERP system version yz.</td>
</tr>
<tr>
<td>Human resources</td>
<td>The availability of human resources from xxx is hard to control since many of the people still have work to do in older projects. Unfortunately, that work has usually a higher priority</td>
</tr>
<tr>
<td>Supplier delivery time dependency</td>
<td>The outsourced application components may be delayed due to plan execution slippery.</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Who is involved in Risk Management?

- Customer
- End-user
- Project Team
- Management
- Product Management
- Related Projects
- Subcontractors and Suppliers

*Risk Management is Communication!*
When?

- Business-Case Analysis for Outsourcing
- Preparation for Outsourcing (Partner Selection, Frame Contracts)
- Status and Briefing of Requirements,
- Detailed Contracts and Project Planning
- Milestones in Project Execution
- Transfer and Maintenance

Risk Management is a Continuous Process!
Generic Risk Management Process

Mandate & Goal

What are the tasks of RM?

Package

What did we learn?

Identify

What can go wrong in my project?

Monitor

What has to be changed?

Describe Risks

What exactly is the risk?

Analyze

What are important risks?

Prioritize Risks

What are the tasks of RM?

Control Planning

What shall we do to reduce severity or avoid risk?

Control Implementation

What is the risk status?

Track

What did we learn?
Risk Analysis Method

- **Describe the Risks**
  - Brainstorming potential risks
  - Walkthrough of the risk identification checklist

- **Analyze and Prioritize Risks**
  - Walkthrough risk sheet and estimate the probability and cost of each risk
  - Calculate risk rating of each risk (e.g. likelihood * consequence)
  - Prioritize in risk classes concentrate on class “High”

---

**Sample Risk Grid**

- **Likelihood Factor**
  - 1 - Low
  - 2 - Minor
  - 3 - Moderate
  - 4 - Significant
  - 5 - High

- **Consequence Severity Factor**
  - 1 - Low
  - 2 - Minor
  - 3 - Moderate
  - 4 - Significant
  - 5 - High

Legend:
- High
- Medium
- Low
## Likelihood

### What Is the Likelihood the Risk Will Happen?

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood</th>
<th>Your Approach and Processes...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not Likely:</td>
<td>...Will effectively avoid or mitigate this risk based on standard practices</td>
</tr>
<tr>
<td>2</td>
<td>Low Likelihood:</td>
<td>...Have usually mitigated this type of risk with minimal oversight in similar cases</td>
</tr>
<tr>
<td>3</td>
<td>Likely:</td>
<td>...May mitigate this risk, but workarounds will be required</td>
</tr>
<tr>
<td>4</td>
<td>Highly Likely:</td>
<td>...Cannot mitigate this risk, but a different approach might</td>
</tr>
<tr>
<td>5</td>
<td>Near Certainty:</td>
<td>...Cannot mitigate this type of risk; no known processes or workarounds are available</td>
</tr>
</tbody>
</table>
### Severity of Consequence / Harm

<table>
<thead>
<tr>
<th>Level</th>
<th>Technical</th>
<th>Schedule</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minimal or no impact</td>
<td>Minimal or no impact</td>
<td>Minimal or no impact</td>
</tr>
<tr>
<td>2</td>
<td>Minor perf shortfall, same approach retained</td>
<td>Additional activities required; able to meet key dates</td>
<td>Budget increase of less than 1%</td>
</tr>
<tr>
<td>3</td>
<td>Mod perf shortfall, but workarounds available</td>
<td>Minor schedule slip; will miss need date</td>
<td>Budget increase of less than 5%</td>
</tr>
<tr>
<td>4</td>
<td>Unacceptable, but workarounds available</td>
<td>Program critical path affected</td>
<td>Budget increase of less than 10%</td>
</tr>
<tr>
<td>5</td>
<td>Unacceptable; no alternatives exist</td>
<td>Cannot achieve key program milestone</td>
<td>Budget increase of more than 10%</td>
</tr>
</tbody>
</table>

Given the risk is realized, what would be the magnitude of the impact?
Risk Mitigation and Contingency Planning

- **List Mitigation Actions**
  - Start with most severe risks
  - List possible actions to reduce probability and/or cost
  - Some risks can be avoided (e.g. avoid a specific requirement)

- **Contingency Planning**
  - Only for the most severe risks that cannot be mitigated
  - List actions to take should the risk materialize
Monitor

- Risks identified as “High” are tracked at the Program Level. The status of each step in the risk reduction plan is updated and reported at the regularly scheduled reviews by the Project Manager.
  - Actions are initiated as required where risk reduction plan activities are not being accomplished.
  - Special briefings of program risks to program management will also be scheduled as needed.

- “Medium” Risks are monitored on Project Management level.

- Re-Assess Risks regularly:
  - Where the taken risk control measures successful? i.e. Likelihood and damage of controlled risks reduced?
  - Did the risk control measures introduce new risks?
  - Additional other risks identified? E.g. through early evaluation with customers. Analyze them.
Supplier Selection Risk Factors

- Supplier selection process / criteria
- Supplier capability evaluation
- Executive (or customer) influence on selection
- Number of supplier candidates
- Selection process documentation
<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Low Risk Cues</th>
<th>Medium Risk Cues</th>
<th>High Risk Cues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supplier Selection Risk Factors</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Supplier selection criteria</td>
<td>organization weighs technical, process and cost implications when selecting supplier</td>
<td>organization advocates mitigating technical and process related risks while selecting low cost supplier</td>
<td>organization expects low cost supplier will be selected</td>
</tr>
<tr>
<td>2 Supplier evaluation</td>
<td>potential suppliers' technical and process capabilities were reviewed by technical</td>
<td>supplier alternatives were reviewed based on questionnaires or other high level materials</td>
<td>supplier capabilities reviewed by a small team of technical experts, who recommended selection without looking at alternatives</td>
</tr>
<tr>
<td>3 End user involvement in supplier eval.</td>
<td>end users were directly involved in evaluation of the supplier</td>
<td>end users reviewed the results of the evaluation</td>
<td>end users were not involved in the supplier evaluation</td>
</tr>
<tr>
<td>4 Executive (or customer) influence</td>
<td>executives have expressed no written or verbal support for any particular supplier</td>
<td>executives have made written or verbal comments favoring a particular supplier</td>
<td>executives have made a written or verbal mandate of a particular supplier or customer has selected the supplier</td>
</tr>
<tr>
<td>5 Number of supplier candidates</td>
<td>several qualified suppliers from which to choose</td>
<td>just a few qualified suppliers</td>
<td>this candidate is the sole potential supplier, thus evaluation is almost irrelevant; or all supplier candidates have poor prior</td>
</tr>
<tr>
<td>6 Selection process documentation</td>
<td>the evaluation and selection process follows an approved, documented organization</td>
<td>the evaluation and selection process were based on external recommendations</td>
<td>no documented evaluation and selection process was used</td>
</tr>
<tr>
<td>7 Evaluation criteria</td>
<td>supplier evaluation criteria consider defined requirements</td>
<td>supplier evaluated using pre-defined evaluation criteria</td>
<td>no evaluation criteria used in supplier selection process</td>
</tr>
</tbody>
</table>
Management of Product Risks

Risk Areas

- IT Security Risks
- Product Safety Risks
Product Safety Risks

- What are possible hazards?
  - Major: May lead to death or serious injury
  - Moderate: Non-serious injury is possible
  - Minor: No injury or damage to health is possible

- Software Risk Management Approach
  - Safe Product
    - All hazards have been addressed
    - Risks have been reduced to acceptable levels
    - Adequate software processes are implemented
    - Process is effective
Hazard identification

- **Software and Product IT-Security hazards** cover Confidentiality, Integrity and Availability aspects, e.g.
  - A medical Instrument can be run with expired maintenance or reagents.
  - Data storage exhausted e.g. harddisk is filled with logfiles
  - Wrong or unclear patient result presentation
  - Timing-, multitasking-, jittering-problems or deadlocks occur
  - Access to patient/personal data for unauthorized people
  - Instruments or databases are accessed by unauthorized persons via the intra- or internet
  - Service passwords are static and become widely known
  - Audit trails and logfiles can be edited
## Product Risk Management

- Same process as for Business or Project Risk Management
- Product Manufacturer is held responsible for
  - Whole product
  - All integrated parts

<table>
<thead>
<tr>
<th>Formal Product Risk Management Process</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inhouse developed software</td>
<td>X</td>
</tr>
<tr>
<td>Outsourced development for the purpose of the product</td>
<td>X</td>
</tr>
<tr>
<td>Software already available (OTSS, legacy code)</td>
<td>Not possible, OTSS already exists</td>
</tr>
</tbody>
</table>
Software Risk Management According to IEC 62304

Risk Assessment

- Critical Harm
- Sequence of critical software events / Causes for harm
- Critical Software Items in Architecture
- Risk Control Measures
  - New Requirement (SRQ)
  - Improved Design
  - SW Item Specification

Risk Control Verification

- Declaration of residual risks
- Test Plans, Unit, Integration, System Testing
- Verification of risk control measurements (effective, Residual risks)
Risk Mitigation Documentation

<table>
<thead>
<tr>
<th>Project stage</th>
<th>Product … Before measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>24-Jan-09</td>
</tr>
<tr>
<td>Risks assessed</td>
<td>49</td>
</tr>
<tr>
<td>Green area</td>
<td>34</td>
</tr>
<tr>
<td>Yellow area</td>
<td>11</td>
</tr>
<tr>
<td>Red area</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project stage</th>
<th>Product … After measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>30-Nov-09</td>
</tr>
<tr>
<td>Risks assessed</td>
<td>49</td>
</tr>
<tr>
<td>Green area</td>
<td>48</td>
</tr>
<tr>
<td>Yellow area</td>
<td>1</td>
</tr>
<tr>
<td>Red area</td>
<td>0</td>
</tr>
</tbody>
</table>

Product Risk Reduction to Acceptable Level

Documentation Of Residual Risks
Off-the-Shelf Software (OTSS)

- Analysis and Documentation during Design:
  - Make vs. Buy Analysis
  - Software Package Selection and Purchasing Control

- Steps
  - Analyze Level of Concern:
    - Worst case hazard severity if software malfunctions:
      - Minor: document hazard mitigation actions
      - Moderate: Describe and justify residual risks (Basic documentation)
      - Major: Special documentation demonstrates risk reduction
OTSS Risk Documentation

- **Basic Documentation**
  - Why the OTSS is appropriate for use in the product
  - Used versions, patches, drivers, …
  - OTSS requirements for the product
  - Testing appropriate for hazards
  - Configuration Management for OTSS deliverables

- **Special Documentation (major hazards)**
  - Provide assurance regarding the OTSS development process by the vendor
  - Demonstrate that vendor’s Verification & Validation are adequate
  - Demonstrate maintenance and support of the OTSS will be adequate