



THE UNIVERSITY OF  
MELBOURNE

SWEN90016  
Software Processes & Project Management

# Risk Management

*Christoph Treude, Andrew Valentine*  
*School of Computing and Information Systems*  
*The University of Melbourne*  
*[christoph.treude@unimelb.edu.au](mailto:christoph.treude@unimelb.edu.au), [andrew.valentine@unimelb.edu.au](mailto:andrew.valentine@unimelb.edu.au)*

1. Understand the fundamentals of risk management
2. Understand the Risk Management Process
3. Understand how to:
  - plan risk management activities
  - identify risks
  - analyze and assess risks
  - respond to risks (risk strategies)
  - monitor and control risks

- Determine which events should be considered as risks by analysing the following:
  - Is the *probability* of the event occurring greater than *zero*?
  - What is the *impact* of the event on the project?
  - Do we have some *degree of control* over the event or its outcome?
- Generic Risks:
  - Threats or opportunities common to every software project (e.g. staff turnover, budget and schedule pressures)
- Product-specific Risks:
  - Threats or opportunities specific to the product, and can only be identified by people who have a clear understanding of the product and technology

- **Project risks**

- Affect the planning of the project  
e.g. Budget, Schedule, Scope, Personnel, etc.

- **Product risks**

- Affect the quality or performance of the outcome being developed  
e.g. Design problems, implementation problems, interface problems, maintenance problems, verification problems

- **Business risks**

- Affect the economic success of the project  
e.g. No demand for product, loss of management support, loss of external funding for the project etc.

- **Risk identification**

- Deals with using a systematic approach for identifying and creating a list of threats and opportunities that may impact the project's goals

- **Risk identification techniques**

- Pondering
- Interviewing
- Brainstorming
- Checklists
- Delphi Technique
- SWOT Analysis

MELBOURNE

- **Pondering**
  - This simply involves an individual taking the “pencil and paper” approach of risk identification, which involves sitting and thinking about the possible risks that could occur in the project
  - This is one of the initial risk assessment tasks used in many projects
- **Interviews/questionnaires**
  - Interviewing project stake holders, or asking them to fill out questionnaires, to harness their knowledge of a domain
  - It is unlikely that a risk manager in a software project will have sufficient knowledge of the methods and tools to be employed to provide a comprehensive view of the risks, so input from stakeholder and domain experts is essential



- Brainstorming
  - The team can use a *risk framework* or the *Work Breakdown Structure (WBS)* to identify threats and opportunities
  - The key is to encourage contributions from everybody
  - The group then discuss and evaluate
- Checklists
  - This involves the use of standard checklists of possible risk drivers that are collated from experience
  - These checklists are used as triggers for experts to think about the possible types of risks in that area

- Delphi Technique
  - A group of experts are asked to identify risks and their impact
  - The responses are then made available to each other anonymously
  - The experts are then asked to update their response based on the responses of others – repeated until consensus is reached
- SWOT Analysis (Case study)
  - Strengths, Weaknesses, Opportunities and Threats
  - This technique allows finding strengths and weaknesses as well



MELBOURNE

- Example: Risk of a third-party software application

Consider the example of using a third-party software application to provide some functionality of a system that is being developed. The third-party application is developed in parallel with the system:

- Risks:

1. The application could be delivered later than planned, thereby delaying the delivery of the entire system.
2. Once complete, the third-party application may not be reliable enough to be used, meaning that a new third-party application providing the functionality will need to be sourced or developed.
3. The third-party application may deliver behaviour that is inconsistent with the expectations of the system developers, meaning that a new third-party application providing the functionality will need to be sourced or developed.

# Identified Risks - example

MELBOURNE

Risk Source Category	Possible Risk Examples /Risk Factors
Project Size and Complexity	<ul style="list-style-type: none"> <li>• Effort Hours</li> <li>• Calendar Time</li> <li>• Estimated Budget</li> <li>• Team and Size (Number of Resources)</li> <li>• Number of Sites</li> <li>• Number of Business Units</li> <li>• Number of Dependencies on other Projects</li> <li>• Degree of Business Change</li> </ul>
Requirements	<ul style="list-style-type: none"> <li>• Volatile Requirements</li> <li>• Unrealistic Quality Requirements</li> <li>• Complex Requirements</li> </ul>
Change Impact	<ul style="list-style-type: none"> <li>• Replacement of New System</li> <li>• Impact on Business Policies</li> <li>• Impact on Organisational Structure</li> <li>• Impact on Systems Operations</li> </ul>

# Identified Risks - example

Risk Source Category	Possible Risk Examples /Risk Factors
Stakeholders	<ul style="list-style-type: none"> <li>• All key stakeholders have not been identified</li> <li>• Missing "Buy-In" from a key stakeholder</li> <li>• Stakeholder needs not completely identified</li> <li>• Key stakeholders not fully engaged</li> </ul>
Organization	<ul style="list-style-type: none"> <li>• Changes to Project Objectives</li> <li>• Lack of Priorities</li> <li>• Lack of Project Management "Buy-In" and Support</li> <li>• Inadequate Project Funding</li> <li>• Misallocation and Mismanagement of Resources</li> </ul>
Scope	<ul style="list-style-type: none"> <li>• Grope</li> <li>• Leap</li> <li>• Creep</li> </ul>
Schedule	<ul style="list-style-type: none"> <li>• Estimated Assumptions are Not Holding True</li> <li>• Scheduled Contingency is Not Adequate</li> <li>• Inadequate or Poor Estimation</li> </ul>

## Stakeholders

2012 – Bank of America started charging its customers \$5 per month to gain access to their funds using their debit cards

No Risk Management Plan – to account for risks stemming from ineffectively managing stakeholder consultations. Consequences far greater than imagined.

5-November-2011 – *Bank Transfer Day*

8-November-2011 – *Dump your Bank Day*

## RESULT

1. Thousands of customers dumped Bank of America and moved away to other banks and credit unions
2. A Risk Management Plan could have saved Bank of America bad press and the loss of business from lots of old time customers

## TAKE AWAY

‘Going full steam’ into a project – without little or no research on potential consequences as key project risks can turn projects into a disaster

[Bank Transfer Day - Wikipedia](#)

[Bank dumping day begins - Nov. 4, 2011 \(cnn.com\)](#)

[Bank Transfer Day - Wikipedia](#)

[Bank dumping day begins - Nov. 4, 2011 \(cnn.com\)](#)



# Risk Management



1. Understand the fundamentals of risk management
2. Understand the Risk Management Process
3. Understand how to:
  - plan risk management activities
  - identify risks
  - **analyze and assess risks**
  - respond to risks (risk strategies)
  - monitor and control risks



[Risk management Jokes \(jokejive.com\)](http://jokejive.com)

MELBOURNE

- Risk analysis and assessment provide a systematic approach for evaluating the risks
- **Risk analysis**
  - Identify each identified risk's *probability* and *impact*
- **Risk assessment**
  - *Prioritize* risks so that an effective *risk strategy* can be formulated
- Two approaches for analysis and assessment:
  - Qualitative: subjective assessment based on experience/intuition
  - Quantitative: mathematical and statistical techniques



- The important steps of risk analysis are:

1. Estimating the *risk probability (P)*

- this is an estimation of the probability that the risk will occur
- usually done based on expert judgement

2. Estimating the *risk impact (I)*

- the impact that the risk will have on the project
- Usually measured in a scale of 1 – 5 (or 10):

(1)no impact; (2) minimal impact; (3) moderate impact; (4) severe impact; and (5) catastrophic impact

- Impact can be expressed as a monetary value

- The important steps of risk analysis cont..

### 3. Compute *risk exposure (or $P * I$ Score)*

$$\text{Risk exposure} = P * I$$

### 4. Identifying the root cause

- It is important that one identifies the root causes of all risks
- If this root cause can be identified, then all of these risks can be controlled by addressing the root cause

MELBOURNE

- Example: Risk of a third-party software application

Consider the example of using a third-party software application to provide some functionality of a system that is being developed. The third-party application is developed in parallel with the system:

- Risks:
  1. The application could be delivered later than planned, thereby delaying the delivery of the entire system.
  2. Once complete, the third-party application may not be reliable enough to be used, meaning that a new third-party application providing the functionality will need to be sourced or developed.
  3. The third-party application may deliver behaviour that is inconsistent with the expectations of the system developers, meaning that a new third-party application providing the functionality will need to be sourced or developed.



# Risk Analysis - Example

MELBOURNE

Risk ID	Risk	Probability	Impact	Exposure
1	The application could be delivered later than planned, thereby delaying the delivery of the entire system.	0.15	\$10,000	\$1500
2	Once complete, the third-party application may not be reliable enough to be used, meaning that a new third-party application providing the functionality will need to be sourced or developed	0.05	\$20,000	\$1000
3	The third-party application may deliver behaviour that is inconsistent with the expectations of the system developers, meaning that a new third-party application providing the functionality will need to be sourced or developed	0.2	\$20,000	\$4000

**Risk Impact Analysis  
Table**

Risk ID	Risk	Probability (0 – 100%)	Impact (1-10)	Exposure (1-5)	Rank
1	A key member leaving the project	40%	4	1.6	4
2	Client unable to define scope and requirements	50%	6	3.0	3
3	Client experiences financial problems	10%	9	0.9	5
4	Response time not acceptable to the user/client	80%	6	4.8	1
5	Technology does not integrate with existing application	60%	7	4.2	2
6	Financial manages deflects resources away from the project	20%	3	0.6	6
7	Client unable to obtain license agreement	5%	7	0.4	7

## Risk Impact Analysis Table

MELBOURNE

- **Risk matrix** - define the level of risk by considering the probability or likelihood consequence severity.
- A mechanism to increase visibility of risks and assist management decision making.

		High		
IMPACT	Medium	Medium	High	High
	Low	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		LIKELIHOOD		

# Risk Matrix - Example

MELBOURNE

IMPACT	High	Risk 3,7	Risk 5	
	Medium		Risk 1, 2	Risk 4
	Low	Risk 6		
		Low	Medium	High
		LIKELIHOOD		



MELBOURNE

Quantitative approaches include mathematical and statistical techniques

- They are based on modelling a particular risk situation - probability distributions of risks are the main consideration
- Common Techniques:
  - Decision Tree Analysis
  - Simulation
  - Sensitivity Analysis

Quantitative approaches are beyond the scope of this subject



1. Understand the fundamentals of risk management
2. Understand the Risk Management Process
3. Understand how to:
  - plan risk management activities
  - identify risks
  - analyze and assess risks
  - respond to risks (risk strategies)
  - monitor and control risks

MELBOURNE

- Shari L. Pfleeger and Joanne M. Atlee. Software Engineering: Theory and Practice. Prentice–Hall International, 3rd edition, 2006.
- R. S. Pressman. Software Engineering: A Practitioner's Approach. McGraw Hill, seventh edition, 2009.
- J.T. Marchewka. Information Technology Project Management. John Wiley & Sons, fourth edition, 2012.