SWEN90016
Software Processes & Project Management

Risk Management

Marion Zalk
Department of Computing and Information Systems
The University of Melbourne
mzalk@unimelb.edu.au

2021 – Semester 2
Lecture 3

Learning Outcomes

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

Learning Outcomes

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

What is a risk?

- **A *risk* is a:**

  Possible future event that has negative results

  Hazard; peril; or exposure to loss or injury

  - Webster's dictionary

  An uncertain event or condition that, if it occurs, has a positive or negative effect on the project objectives

  - PMBOK

- The first two definitions above treat risk and always negative, whereas the third definition considers positive as well as negative impacts - *opportunities* (we will stick with the third definition)

Risk vs Uncertainty

- Risk is different to uncertainty although they are related.

- ***Uncertainty:***
  - Lack of complete certainty about an event/outcome
  - The event/outcome has a probability of less than 1
  - E.g. outcome of a sporting event
- ***Risk:***
  - Uncertainty that has an impact
  - E.g. If you have placed a bet on the sporting event, or have some other personal stake in it, then there is risk associated with the outcome of the sporting event

Risk is a result of uncertainty but not every uncertainty is a risk.

Why formal Risk Management

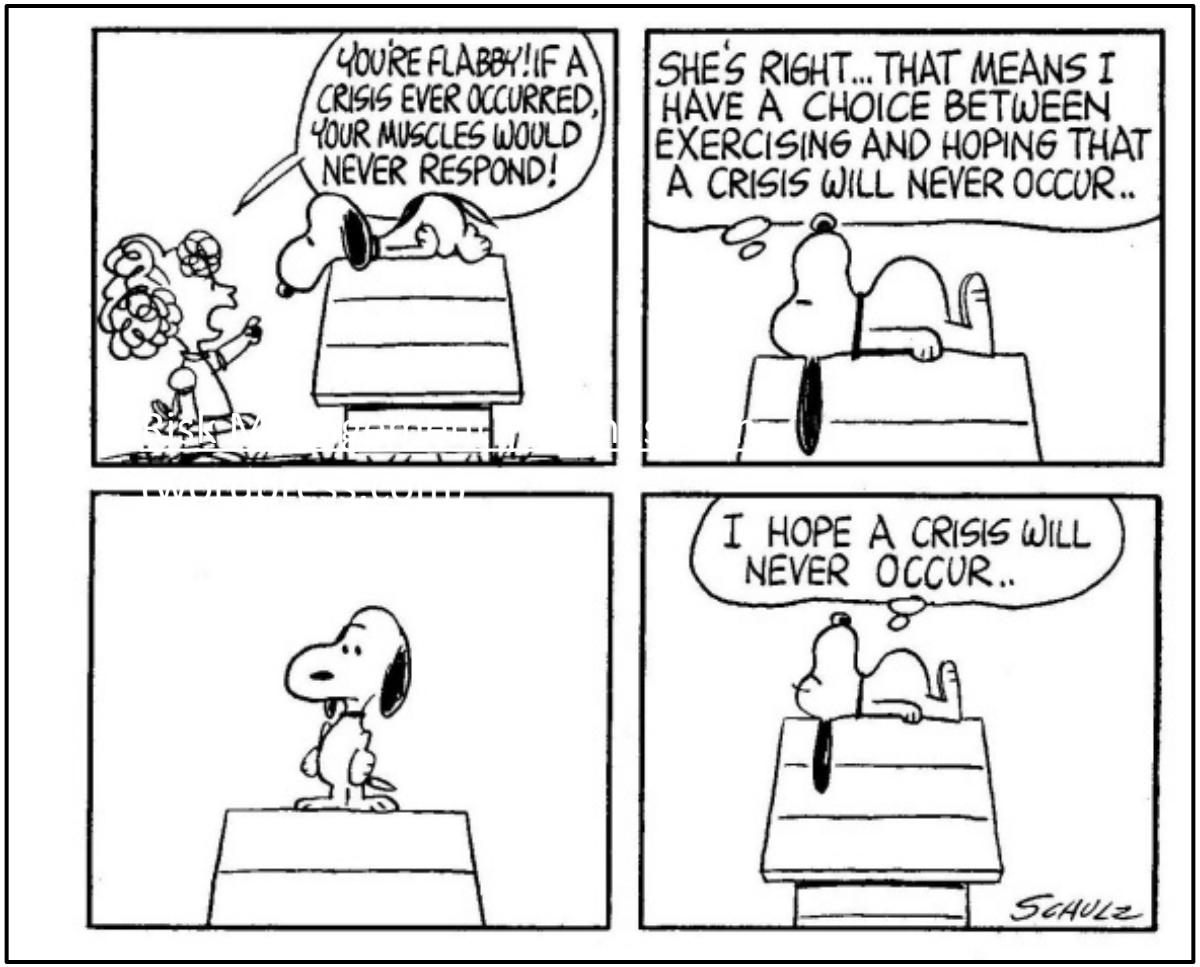
- We deal with risks in our lives every day
  - e.g. Planning to get to the lecture

- Projects have many possible risks, that could have significant impacts on the outcomes:
  - Business risks
  - Project risks
  - Product risks
- A planned Risk Management process is essential
- The goal of project risk management is to:

  minimising the impact of potential negative risks while maximising the impact of potential positive risks

Learning Outcomes

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 | Beings Akin

Risk Management Process

Risk Management Process

- **Plan**
  - How to approach and plan risk management activities?
- **Identify**
  - Identify the possible risks
- **Analyse and Assess (Qualitative and Quantitative):**
  - Identify the relative priorities of the identified risks
- **Respond (Action):**
  - How can we reduce the likelihood or impact of risks?
- **Monitor and Control:**
  - How can we detect the ongoing status of our risks? How can we control them effectively and efficiently?

Learning Outcomes

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 Planning

- The output of risk management planning is a ***Risk Management Plan (RMP)*** that documents the procedures for managing risks throughout a project

- The project team should review the RMP and understand and implement the organisation's and the sponsor's approaches to risk management

- The level of detail will vary with the needs of the project

Risk Management Plan Template

- The Risk Management Plan
  - Methodology
  - Roles and Responsibilities
  - Budget and Schedule
  - Risk Categories
  - Risk Probability and Impact
  - Tracking
  - Risk Documentation
  - Contingency Plans
  - Fall-back Plans

Learning Outcomes

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

Characteristics of Risk

- 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

Kinds of Risk

- **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

- **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

Risk Identification Techniques

- 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

Risk Identification Techniques

- 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

Risk Identification Techniques

- Delphi Technique
  - A group of experts are asked to identify risks and their impact
  - The responses are them 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

Risk Identification - Example

- 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

Risk Source Category	Possible Risk Examples /Risk Factors
Project Size and Complexity	• Effort Hours • Calendar Time • Estimated Budget • Team and Size (Number of Resources) • Number of Sites • Number of Business Units • Number of Dependencies on other Projects • Degree of Business Change
Requirements	• Volatile Requirements • Unrealistic Quality Requirements • Complex Requirements
Change Impact	• Replacement of New System • Impact on Business Policies • Impact on Organisational Structure • Impact on Systems Operations

Identified Risks - example

Risk Source Category	Possible Risk Examples /Risk Factors
Stakeholders	• All key stakeholders have not been identified • Missing "Buy-In" from a key stakeholder • Stakeholder needs not completely identified • Key stakeholders not fully engaged
Organization	• Changes to Project Objectives • Lack of Priorities • Lack of Project Management "Buy-In" and Support • Inadequate Project Funding • Misallocation and Mismanagement of Resources
Scope	• Grope • Leap • Creep
Schedule	• Estimated Assumptions are Not Holding True • Scheduled Contingency is Not Adequate • Inadequate or Poor Estimation

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)

Risk Management

Learning Outcomes

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)

Risks Analysis and Assessment

- 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

Risk Analysis - Qualitative

- 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 monitory value

Risk Analysis - Qualitative

- 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

Risk Analysis - Example

- 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

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

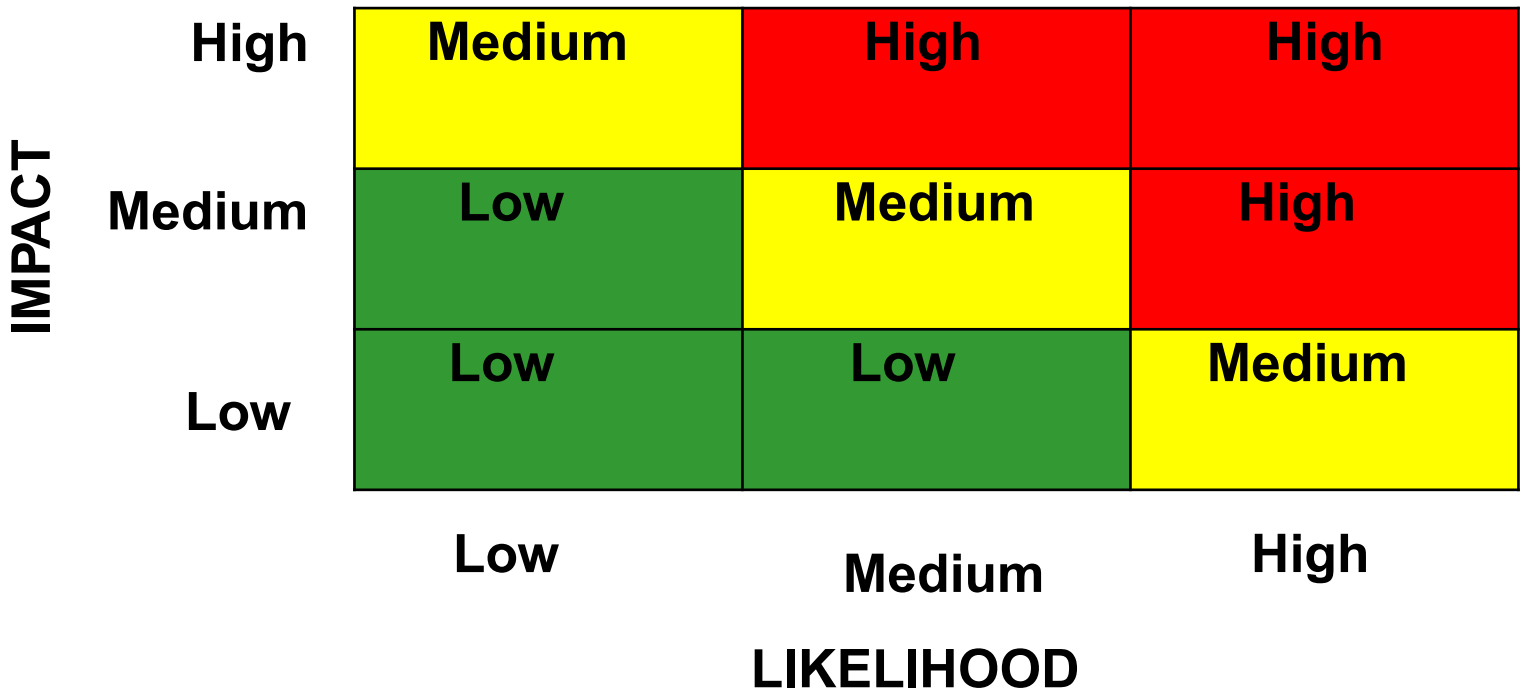
Risk Analysis - Example

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

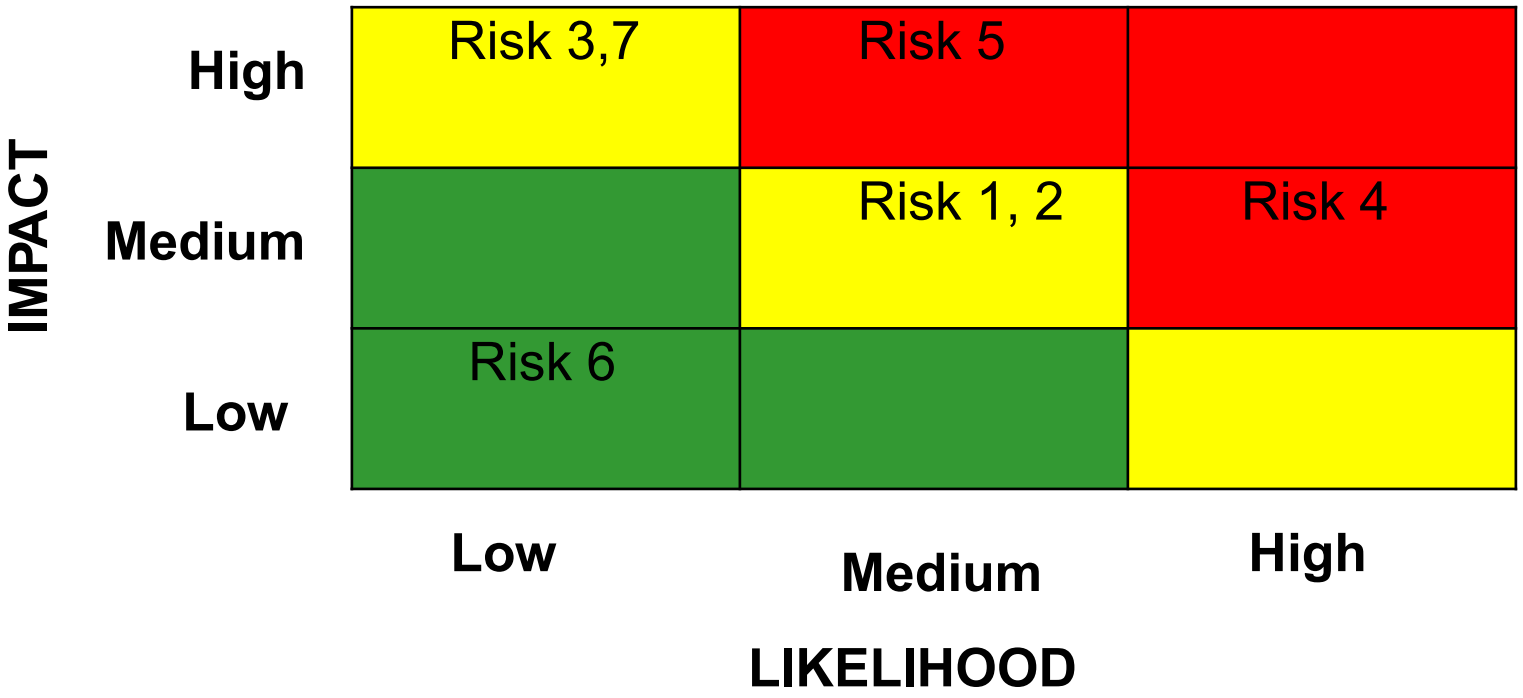
Risk Impact Analysis Table

Risk Assessment – Risk Matrix

- ***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.



Risk Matrix - Example



Risk Assessment - Quantitative

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

Learning Outcomes

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

Respond to Risks

- Purpose of risk analysis and assessment is to identify what opportunities and threats *should be addressed*
- It is not feasible (or advisable) to respond to every threat or opportunity because this requires *resources,* which are usually diverted from the project, which could have more negative impacts on the project
- Therefore, it is important to select appropriate response strategies

Risk Response Strategies

- Four common strategies to handle *threats:*

1. Accept or Ignore

   This means that we believe that the risk is of an acceptable exposure, that we hope that the event does not occur, or that the risk exposure is less than the cost of any techniques to avoid, mitigate, or transfer it.

2. Avoid

   This means that we completely prevent the risky event from occurring, by either ensuring its probability is 0, or ensuring its impact 0.

Risk Response Strategies

- Four common strategies cont..

3. Mitigate

   This involves employing techniques to reduce the probability of the risk, or reduce the impact of the risk. This results in a residual risk — that is, a risk consisting of the same event, but with a lower probability/impact, and therefore low exposure. We then must analyse the residual risk as we would our primary risk.

4. Transfer

   This involves transferring the burden of the risk to another party. Insurance is one example of risk transfer, in which the impact of the risk is offset by payments from the insurer. Another example is outsourcing a portion of the work to somebody with more knowledge and expertise, which comes at a cost.

Risk Response - Example

- 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.

Strategy	Response
Ignore	Do nothing because the vendor is reliable and have delivered quality software in the past.
Avoid	Developing the required functionality in house, rather than buying it or change the requirements so that the functionality is not required at all.
Mitigate	Make the request date well before the required date. We can also reduce the impact of the risk by designing the system such that the third-party application is accessed via a standard interface, and by producing a dummy implementation of that interface that allows development to continue if the third-party application is delivered late.
Transfer	Specifying in the contract that any costs resulting from late delivery of the system will be paid for by the vendor of the third-party application.

Risk Response Strategies

- Four common strategies to handle *opportunities*:
  1. Exploit:

     Add work or change the project to make sure the opportunity occurs

  2. Enhance:

     Increase the probability and positive impact of risk events

  3. Share:

     Allocate ownership of opportunity to a third-party

  4. Accept

     This means that we believe that the cost to exploit or enhance is not justifiable so do nothing about it.

Risk Response Plan

- Once risks and strategies are identified, they can be documented as a part of a risk response plan, also called a Risk Register.
- Template of a simple risk register
  - Risk ID: a unique identification for the risk
  - Trigger: the trigger that flags that the risk has occurred
  - Owner: the person or group responsible for monitoring and responding
  - Response: the strategy for responding
  - Resources: required resources

Risk ID	Trigger	Owner	Response	Resources Required

Risk Register

Learning Outcomes

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

Monitor and control risks

- Once the risk response plan has been created, triggers must be monitored to keep track of various project risks
- New threats and opportunities may arise in the course of the project – they must be identified, analysed and responded to
- Risk monitoring must be part of the overall monitoring and control of the project

Monitor and control risks

- Tools for monitoring and controlling:
  - Risk Audits:
    - external team looks at comprehensiveness of the identification process and ensuring other procedures and processes are in place
  - Risk Reviews:
    - internal reviews of risks periodically that result in status reports generated for PM and those who need-to-know
  - Risk status meetings:
    - risks must be reviewed and discussed in project status meetings, which are periodically held in projects (e.g. weekly meetings)

December 2008 - Manage By Walking Around | Risk management, Manager humor, Risk analysis (pinterest.com.au)

Risk Management Process

Learning Outcomes

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

References

- 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.