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, andrew.valentine@unimelb.edu.au

Copyright University of Melbourne 2021-2023

2023 – Semester 1
Week 3, Module 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

4. Agile SDLC Risk Management

5. Risk Statement – Examples

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.

1. 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.

3. 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

4. Agile SDLC Risk Management

5. Risk Statement – Examples

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

4. Agile SDLC Risk Management

5. Risk Statement – Examples

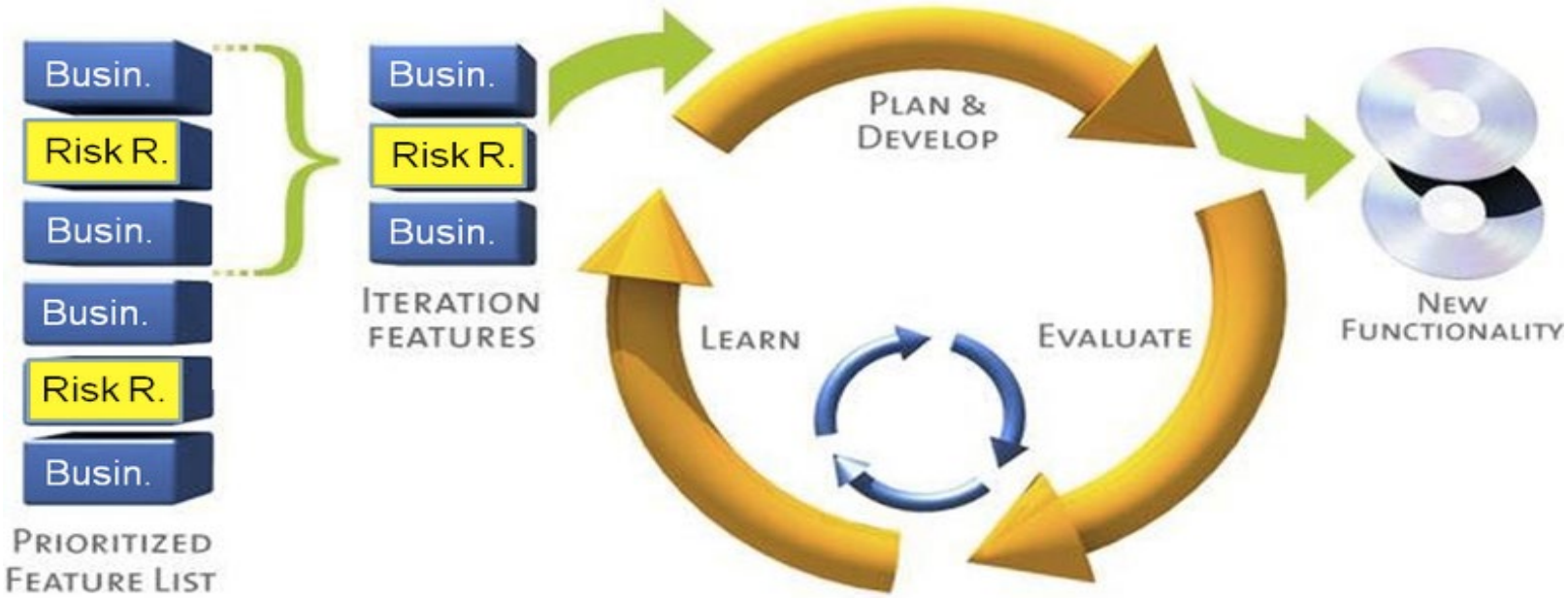
Agile SDLC Risk Management

Identify – capture risks in Risk Register

Analyze – Product Backlog groomed, and priority given to all User Stories, including those which capture risk

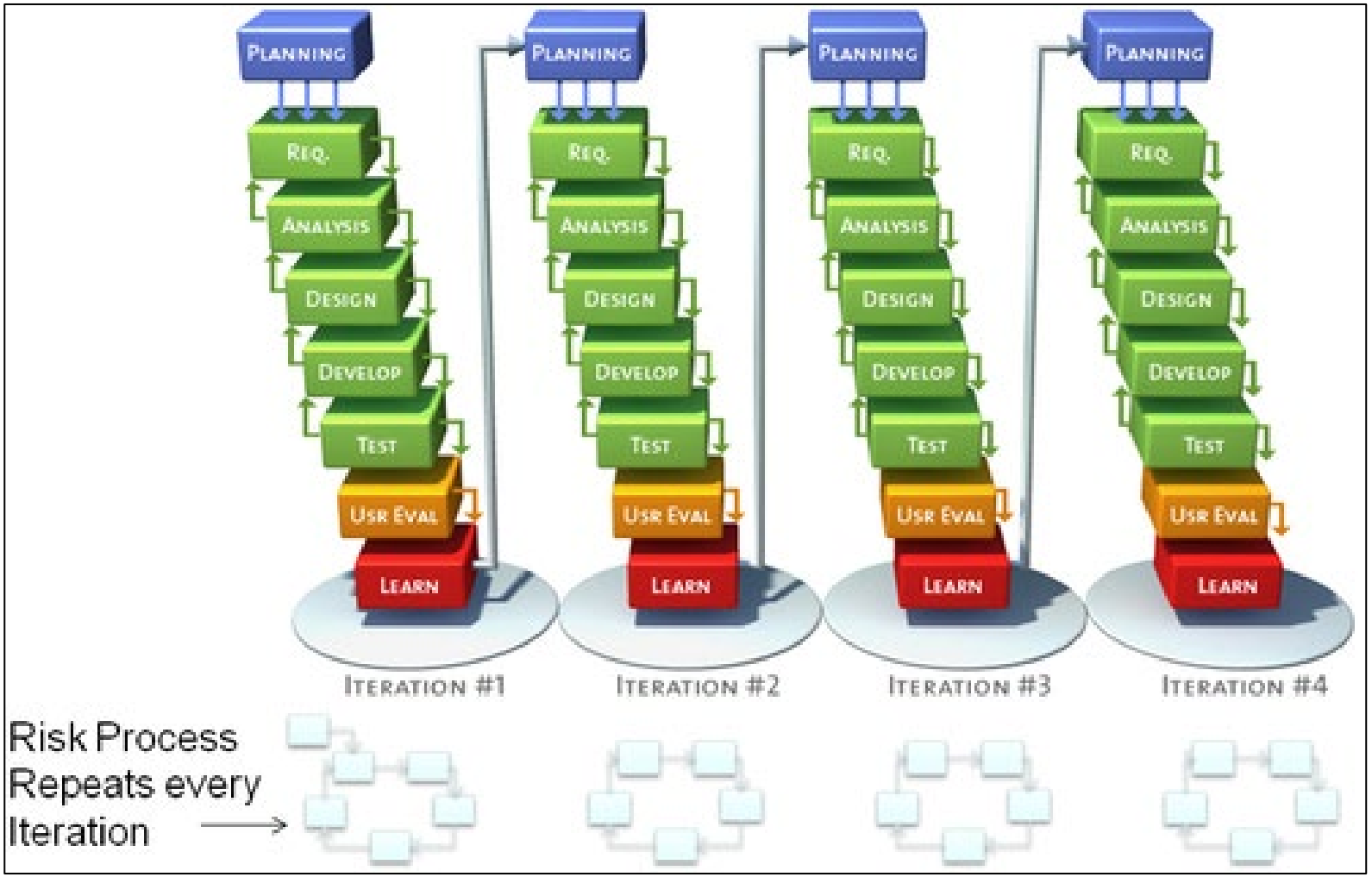
Respond - Mitigate risk in the Sprint

Monitor – During sprint Review, Retrospective & Planning



Picture Courtesy: Agile Risk Management – Leading Answers

Agile SDLC Risk Management



Picture Courtesy: Agile Risk Management – Leading Answers

Agile SDLC Risk Management

Sprint Review risk evaluation

- Build small piece of working software with minimal features
- Showcase the product chunk to the stakeholders ***early***
- Fail ***fast*** and as cheaply as possible, & get timely feedback
- Capture the ***risk item*** in the Product Backlog
- The Product Owner sets the priority of the ***risk item***

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

4. Agile SDLC Risk Management

5. Risk Statement – Examples

Risk Statement - Bad examples

Scope is ill-defined

Statement of fact, not a description of uncertainty

The project may be late

General statement of outcome. Describes no specific risk

Project estimates are very optimistic

Statement. If true, it is an issue and not a risk

Poor data quality

Unqualified Statement.

Risk of project failure is high

Vague. No information on factors that could cause failure

Project could face unexpected issues

Vague. No information on specific issues that creates a risk

Risk Statement - Good example 1

Risk Statement should state the following

ACTION – **CONSEQUENCE** – **IMPACT**

A critical team member becoming unavailable due to illness may create a delay in completing user stories and meeting sprint goals, thereby causing delays in project delivery and potential cost overruns

A critical vulnerability discovered in a third party software library used in the project could lead to security of data being compromised, leading to loss of business to the organization

Risk Statement - Good example 2

Risk Statement should state the following (alternate style)

EFFECT – CAUSED BY – CONSEQUENCE

Delays in development of a critical software module due to challenges of integrating a new third-party software could result in potential impact on end product quality

Reduced user adoption of the product due to poor user interface design testing could cause the project to fail

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

4. Agile SDLC Risk Management

5. Risk Statement – Examples

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.