MONASH University

FIT 3161 – FIT 3163

CS – DS, Software Project 1

Software Development Project Management

Week 5 : Risk Management

Semester 2, 2023

Faculty of Information Technology

Lets check a few things first!

… Recall from week 2: What is a **Project**?

"A project is a temporary endeavour undertaken to create a unique product, service, or result"
(PMBOK® Guide, Sixth Edition, 2017)

Better: *"A project is a temporary endeavour undertaken to create a unique product, deliver a unique service, or achieve a unique result"*

Endeavour → attempt → ***degree of uncertainty → risk → difficulty (→ failure?)***

Commonly accepted understanding of Risk

What is a risk?

”… the ***possibility*** *of something bad happening at* ***some time in the future****; a situation that could be dangerous or have a bad result”*[1]

Examples: ”… risk of losing data”

“… risk of catching Covid19”

[1]https://www.oxfordlearnersdictionaries.com/

Project Risk v/s Software Usage Risk

Need to clearly distinguish between:

1) *Risks relating to* ***Software Development Project,*** *ie occurring during Software Project phase*

And

2) *Risks relating to* ***usage of Software*** *by end user <u>after</u> completion of project and delivery to Client (fulfilment of software development contract)*

In following slides → mostly concerned with ***Software Development Project Risks****, however there often are overlapping considerations*

Risks in Project Management context

All Projects have risks!

*Risks can be associated to a positive outcome, or a better than expected result → **Positive Risks.***

***Positive Risks** = **Opportunities** in more conventional language understanding*

Examples of Positive Risks:

"risk of overestimating the time required to implement a function"

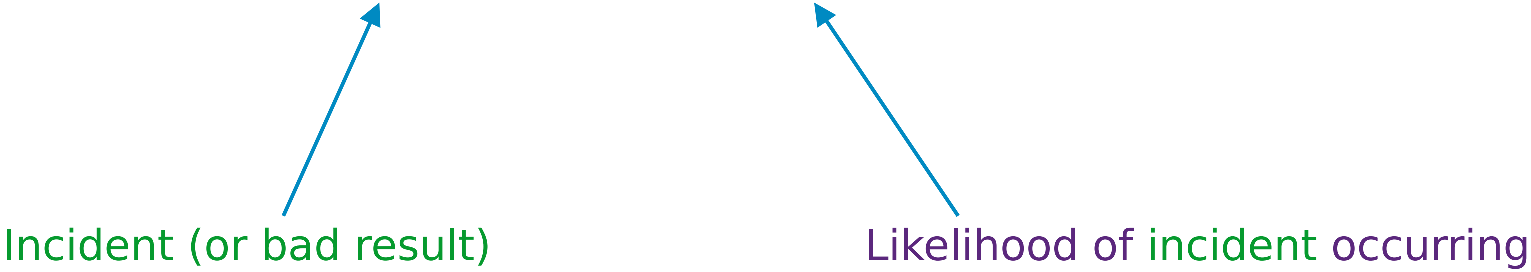
"(business) risk of website getting more hits than expected"

Risk Management

Risk expressed as: Risk of <something happening> in the future

Consider the following risk:

Risk of losing data = Chance of data being lost in the future



Incident (or bad result)

Likelihood of incident occurring

Risk Management is managing both incident and likelihood

(For positive risks, incident = event)

Risk Management

Risk Type	Likelihood Management	Incident Response
Negative	Specify how to **reduce** the **chance** of incident occurring or reduce impact of incident **before** it is triggered	Specify how to rectify or minimize **impact** of incident **after** it is triggered
Positive (Opportunity)	Specify how to **improve** the **chance** of opportunity event arising **before** it happens	Specify how to respond to opportunity if/when event arises.

Note:

1. It is difficult to “improve the chance of opportunity arising”, as this would usually imply that the starting Project plan is too conservative and is potentially wasting project resources. And factors leading to opportunities arising are often outside of the control of Project Managers.

2. It is still important to recognise where positive risks exist and when they are triggered.

Risk Management

1. ***Identify*** *potential incidents that may occur*
2. ***Analyse*** *incident and determine potential impact*
3. ***Determine likelihood*** *(probability) of incident occurring*

Use:

- ***Brainstorming***(*) ` *(Team Members and other stakeholders may participate)*
- ***Interviewing***(*) *(Interview stakeholders)*
- ***SWOT analysis***(*) *(SWOT Analysis may identify Positive Risks)*
- Delphi Technique *(Approach based on repeated Q&A rounds with written responses aiming at reaching consensus between participants/stakeholders)*

(*)These are more appropriate for Student Projects

Risk Qualitative Analysis: Probability-Impact Matrix

Example:

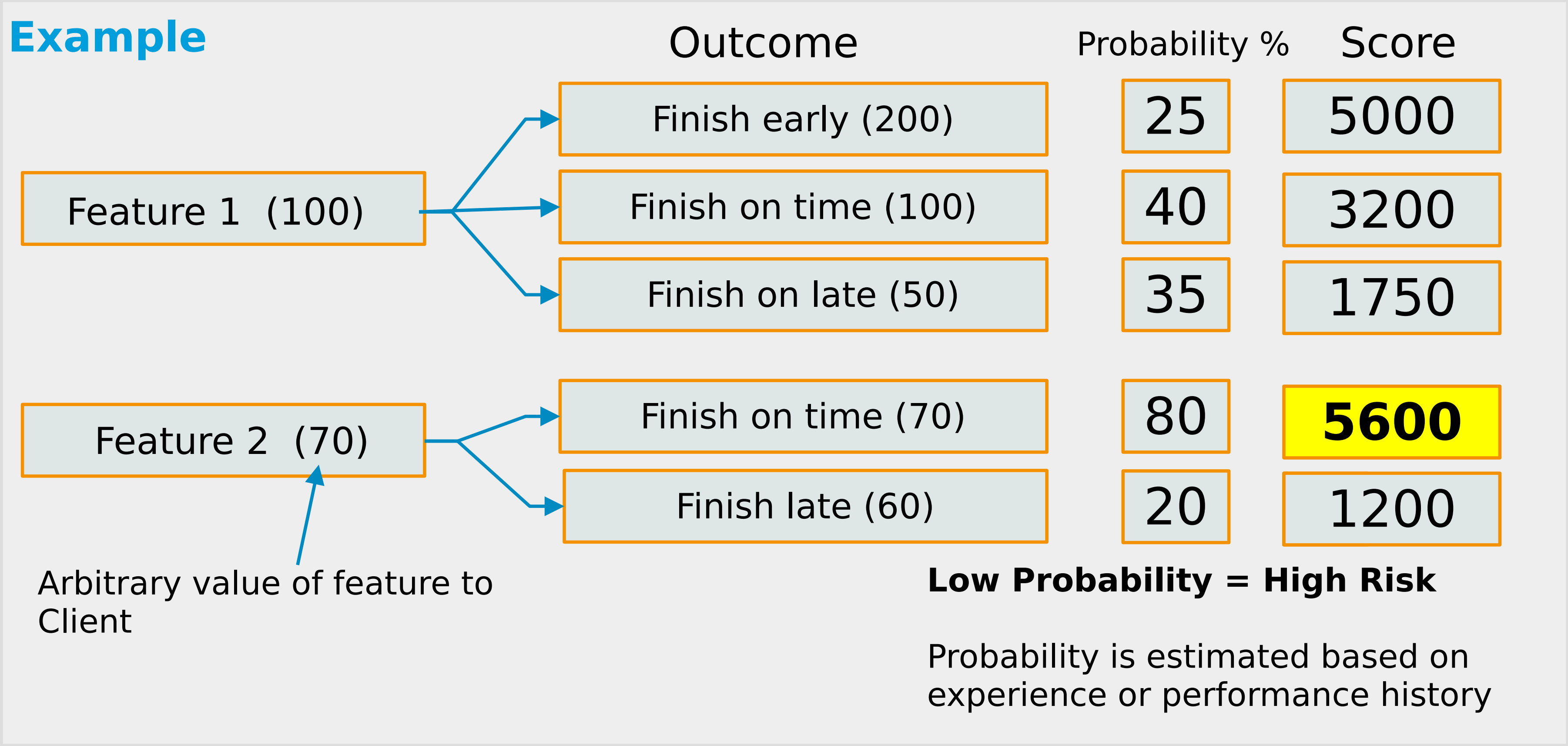
Risk Probability

High	Risk 3 Risk 4	Risk 10	Risk 5 Risk 1
Medium	Risk 9	Risk 7 Risk 8	
Low		Risk 2	Risk 6
	Low	Medium	High

Risk Impact

Risk Quantitative Analysis

Attribute numeric values to features on completion and probability.



Example

Feature	Outcome	Probability %	Score
Feature 1 (100)	Finish early (200)	25	5000
	Finish on time (100)	40	3200
	Finish on late (50)	35	1750
Feature 2 (70)	Finish on time (70)	80	**5600**
	Finish late (60)	20	1200

Arbitrary value of feature to Client

Low Probability = High Risk

Probability is estimated based on experience or performance history

Risk Quantitative Analysis

Conclusion from analysis

- *In previous example , even though Feature 1 is of much higher value to the Client, it is better to take a small risk and to aim to finish on time Feature 2, which is of lesser value. There is also little value in finishing Feature 1 late, even if it is a low risk.*

- *However if the value of finishing Feature 1 ahead of time was higher (say 300), then it would have been better to focus on finishing Feature 1 ahead of time.*

- ***Stakeholder consultation** is required in determining the relative values and in the decision process.*

Risk Response Strategies: TARA(E)

Transference: Share Risk with other people or organisation
Eg, delegate implementation of security features to a Security Experts team.
(Insurance is a classic form of Risk Transference in general)

Avoidance: Do not do what is risky!
Eg, Do not store sensitive data on untrusted storage

Reduction (or Mitigation): Take measures to reduce the likelihood of “bad result” occurring. Eg, if using a new software library to improve expected performance of software (eg: ML Library), ensure new software library is well tested, and training in its use is completed.

Acceptance: As it says!! Accept the risk and the consequence. Eg, in earlier example, accept that a late completion will deliver lower outcome.

Escalation: Similar to Transference, except that transfer is to higher level within same Organisation. Eg, seek advice from “higher up” and implement suggested response.

Note: **Risk Escalation** is not always mentioned in the literature.

Risk Response …

Risks can still exist after responses have been implemented.

- **Residual risk:** Smaller risk still exist after mitigation
  - Eg, In using new Software Library, not all performance issues may have been resolved, and
- **Secondary risk:** New risk introduced as a result of risk response
  - Eg, Transference to Security Expert may increase the risk of going over time
- **The above need to be analysed in overall Risk Management Plan**

Incident Response …

Recall:

Risk Management → Manage likelihood of incident occurring

and also → Manage the incident if/when it is triggered

Incident Response categories:

Contingency Plan: Predefined action to undertake if incident is triggered
Eg: Data is lost → restore data from backup

Fallback Plan: action undertaken if original risk mitigation is not effective; usually planned for high impact incident. This is your **Plan B**
Eg: identify a second source of data if data is lost

Workaround: unplanned and unexpected response when no contingency plan exist for a risk that was not recognised but has triggered.

Risk Register

*A **Risk Register** is a document that summarises the Risk Management Plan in an easy to read and accessible table format.*

*It is a tool for **documenting risk events** and related information*

*It is a **living document** that needs to be reviewed and updated throughout the duration of the project**.***

Risk Register Content

1) *Risk Identification → an ID for a risk, eg: R1*

2) *Risk Description → describes the incident*

3) *Risk Root Cause → What is the cause(s) of the incident*

4) *Risk Trigger → What are the indications that an incident has happened?*

5) *Risk Response Strategy → see TARA(E)*

6) *Risk Incident Response → incident response actions*

Risk Register content (contd…)

6)Risk Owner → Who is responsible to monitor and manage the risk

7)Risk Probability → What is the probability of risk triggering

8)Risk Impact Score → What is the impact of the incident/event expressed as a score (relative to other risks)

9)Risk overall Score = Probability x Impact score

10)Risk Status : eg: Monitored / Triggered / Resolved / Lapsed

11)Last Update → Date when register entry was last updated

Risk Register Example

Risk ID	Description	Root Cause	Trigger	Risk Response
R5	Programmer failing to complete task on time	Programmer lacks experience in program. language used or is work over-committed	Missed complet-ion deadline	Provide training and support to Programmer at start of project. Ensure task is within Programmer abilities. Closely monitor Programmer's progress. Adjust Prog. Work load.
R6	Losing data	Using unreliable storage media/ hardware	Program is producing incorrect result or malfunction	Check quality of storage media and implement live data storage redundancy techniques (eg automatic database replication)

For display Risk Register table is split over 2 slides and continues on next slide ...

Risk Register Example (table continued from previous slide)

Risk ID	Incident Response	Owner	Prob.	Impact Score / 10	Overall Score	Risk Status	Last Update
R5	Allocate new experienced programmer to programming task. Reallocate work load.	Project Manager: J Smith	60	7	420	Monitored	10/10/2022
R6	Restore data from backup and re-do latest and missing data updates.	Database Manager: P Jones	20	10	200	Monitored	28/11/2022

Comment: (Adding a comment in the RR can be useful)

R5 is a risk where the probability may be reduced as the project progresses. The impact however may be higher in late stages of the project as final submission deadline approaches. These changes need to be reflected by updating the register.

Risk Register Top 10 Risks:

1) ***In Risk Register→ re-order risks in order of overall score, with highest score at the top.***

2) ***The Top Risks (typically 10) are <u>monitored more intensively</u>.***

3) ***Risks may enter or fall out of Top list during project execution when risk register is reviewed.***

Risk Status: example scheme

Risk Status *indicates the status of a risk at a time****.***

They need to be monitored and updated. Risk status can change from

- ***Monitored*** ***→ Triggered → ****back to* ***Monitored***
- ***OR Monitored → Triggered → Resolved or Lapsed***

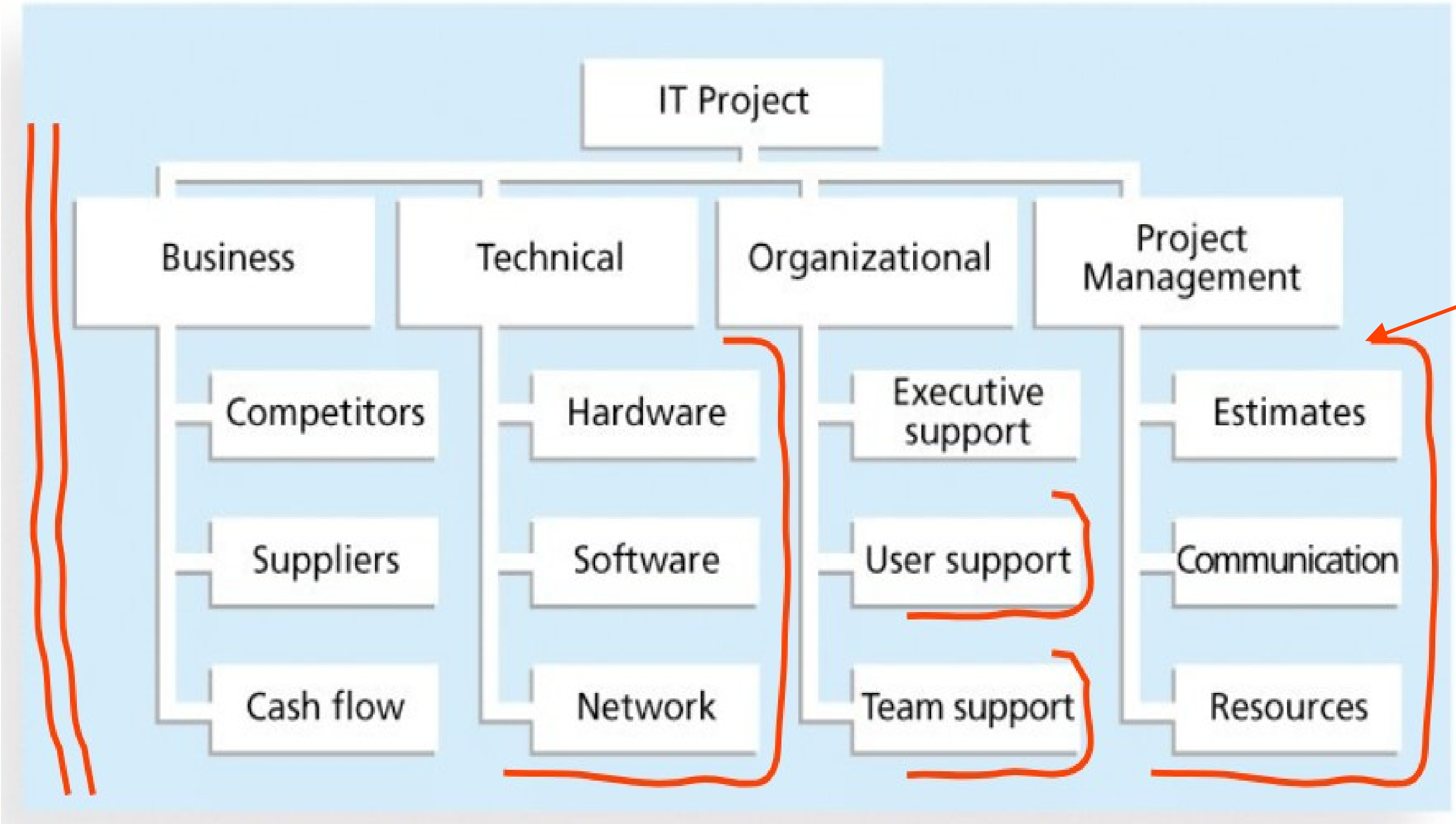
A Resolved Risk *may be Monitored again later*

A Lapsed Risk *does not exist anymore and is documented as such for reference purposes*

Different Organisations may adopt a different Status scheme most suitable to their particular circumstances.

Risk Break Down Structure

Risks can be organised as a Risk Breakdown Structure:



More relevant to Student Project

Each block represents a particular risk area and can have a separate Risk Register. This can be viewd as a form of Risk Transference and hence better Risk Management.

Source: Schwalbe K (2015), Introduction to Project Management 8ed

Conclusion: Good Risk Management

- *Good Risk Management is NOT Crisis Management!*
- *Good Risk Management should prioritise on avoiding Crisis over resolving Crisis.*
- *Risk Management potentially saves time v/s Crisis Management wastes time.*
- *Good Risk Management can go unnoticed → this can lead to its importance being downplayed.*

Break!

Activity: Risk Management

- *Consider your activity “Travelling from home to the university campus”*
- *Write 2 or 3 risk entries in the risk register for this activity*

- *Consider a very small “Hello_World.py”* ***project***
- *Write 2 or 3 risk entries in the risk register for this project*