Chapter 7: Risk Management

Project Management

Afnan Albahli

Risk Definition

Definition of Risk:

- 'an uncertain event or condition that, if it occurs has a positive or negative effect on a project's objectives'.

- 'the chance of exposure to the adverse consequences of future events'.

Risk Key Elements

- **It relates to the future.**
– The future is uncertain.
– Some things that seem obvious when the project is over, might not have appeared obvious during planning (e.g. technology used, project estimation).

- **It involves a cause and an effect.**
– **Causes:**
  - The use of untrained staff.
  - Poor specifications.
  - An inaccurate estimate of effort.
– **Effects:**
  - Cost over run.
  - Low productivity.

Exercise

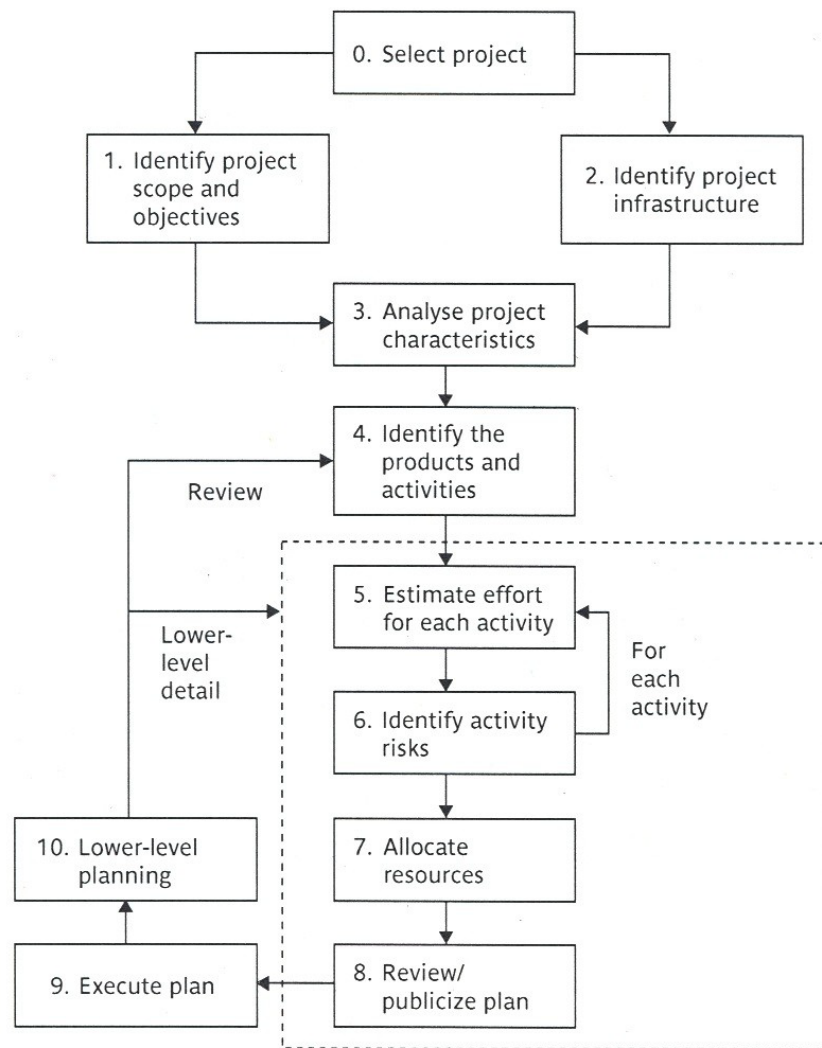**Match the risk cause to the risk effect(s).**

Causes:

a) Staff inexperience.

Effects:

I. Testing takes longer than planned.

II. Planned effort and time for activities exceeded.

III. Project scope increases.

IV. Time delays in getting changes to plans agreed.

Boundaries of Risk Management

- Every plan is based on assumptions and **risk management** tries to plan for and control the situations where those assumptions become incorrect.

- **Risk planning** is carried out at steps: 3 & 6.

Risk Categories

- **Project Risks:** are risks that could prevent the achievement of the objectives given to the project manager and the project team.
- These objectives are formulated toward achieving project success.
- **Project success factors:**
  - On time.
  - Within budget.
  - Required functionality.
  - Quality.
- **Project risks can be classified under these four categories.**

Risk Categories (cont'd)

A different way to categorize risks:

- A sociotechnical model proposed by Kalle Lyytinen and his colleagues
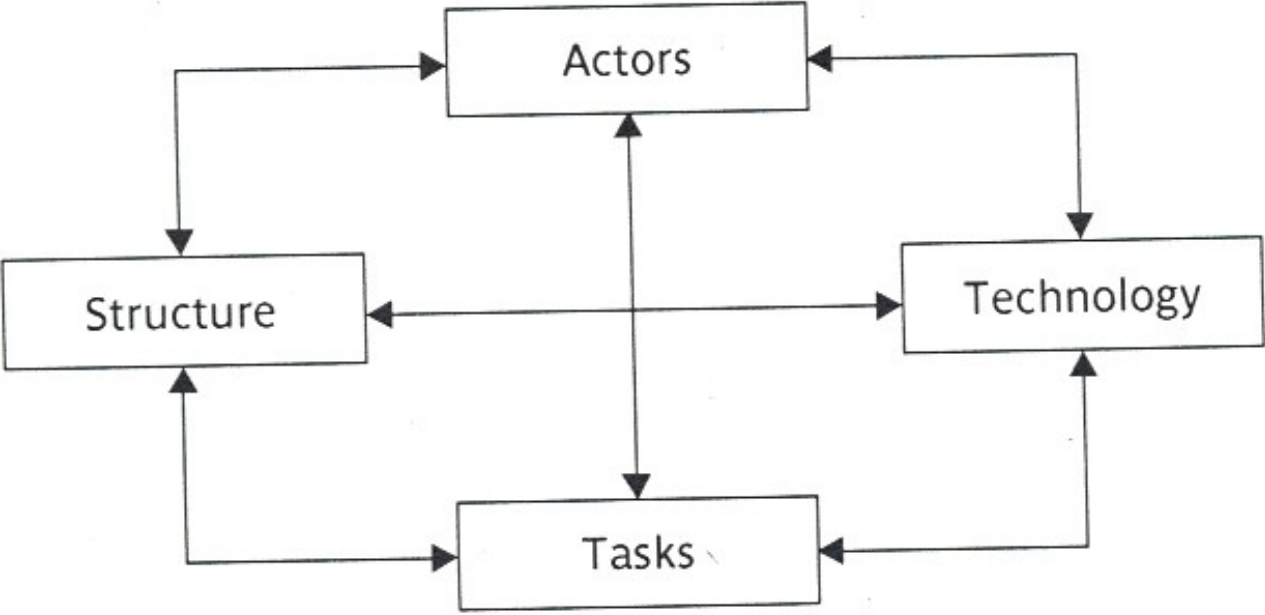
Risk Categories (cont'd)

- **Actors :** refers to all people involved in the development of the application.
- **Risk:**
  - A high staff turnover, leads to expertise of value to the project being lost.
- **Technology:** encompasses both the technology:
  - Used to implement the application and
  - That embedded in the delivered products.
- **Risk:**
  - Relating to the appropriateness of the technology and
  - The possible faults in it.

Risk Categories (cont'd)

- **Structure:** describes the management structures and systems, including those affecting planning and control.

- **Risk:**
  - Responsibility for managing the users involvement at the implementation stage might not be clearly allocated.

- **Tasks:** relates to the work planned.
- **Risk:**
  - The complexity of work might lead to delays because of the additional time required integrate the large number of components.

Risk Framework

Planning for risk includes these steps:

    1. Risk identification.

    2. Risk analysis and prioritization.

    3. Risk planning.

    4. Risk monitoring.

- When risks are identified, plans can be made to reduce or remove their effects.
- The plans are reassessed to ensure:
  - That the original risks are reduced sufficiently and
  - No new risks are inadvertently introduced.

Risk Identification

The two main approaches to identify risk are:

- The use of checklists.
- Brainstorming.

Checklists: are lists of the risks that have been found to occur regularly in software development projects.

• Those checklists often suggest some potential countermeasures for each risk.

• A group of representatives for a project examines a checklist identifying risks applicable to their project.

• PRINCE2, recommends that after completing a project, all the problems that were identified as risks during the project to be added to an organizational risk checklist to be used with new projects.

Software Project Risk Checklist Example

Risk	Risk reduction techniques
Personnel shortfalls	Staffing with top talent; job matching; teambuilding; training and career development; early scheduling of key personnel
Unrealistic time and cost estimates	Multiple estimation techniques; design to cost; incremental development; recording and analysis of past projects; standardization of methods
Developing the wrong software functions	Improved software evaluation; formal specification methods; user surveys; prototyping; early user manuals
Developing the wrong user interface	Prototyping; task analysis; user involvement
Gold plating	Requirements scrubbing; prototyping; cost–benefit analysis; design to cost
Late changes to requirements	Stringent change control procedures; high change threshold; incremental development (deferring changes)
Shortfalls in externally supplied components	Benchmarking; inspections; formal specifications; contractual agreements; quality assurance procedures and certification
Shortfalls in externally performed tasks	Quality assurance procedures; competitive design or prototyping; contract incentives
Real-time performance shortfalls	Simulation; benchmarking; prototyping; tuning; technical analysis
Development technically too difficult	Technical analysis; cost–benefit analysis; prototyping; staff training and development

Risk Identification (cont'd)

Brainstorming (thinking ahead):

Representatives of the main stakeholders of the project, are brought together , in order to use their individual knowledge of different parts of the project

➔ to identify the problems that can occur (identify risks).

Risk Assessment
(Risk analysis and prioritization)

In order to prioritize the risks that were identified, we need a way to distinguish:

- The likely and damaging risks from those identified in the previous step "risk identification".

One way of doing so is to calculate the **risk exposure** for each risk identified, using the following formula:

- *Risk Exposure (RE)= (potential damage) ×(probability of occurrence)*

Risk Assessment (cont'd)

Ways of assessing the potential damage and probability of occurrence:

1. In money values and probabilities.

Say a project depended on a data center vulnerable to fire. It might be estimated that if fire occurred a new computer configuration could be established for $**500,000.** it might also be estimated that there is a **1 in 1000** chance that a fire will occur.

The **risk exposure (RE) in this case would be:**

500,000 *0.001=$500

***The higher the *RE, the more attention or priority is given to* the risk**

With some risks:
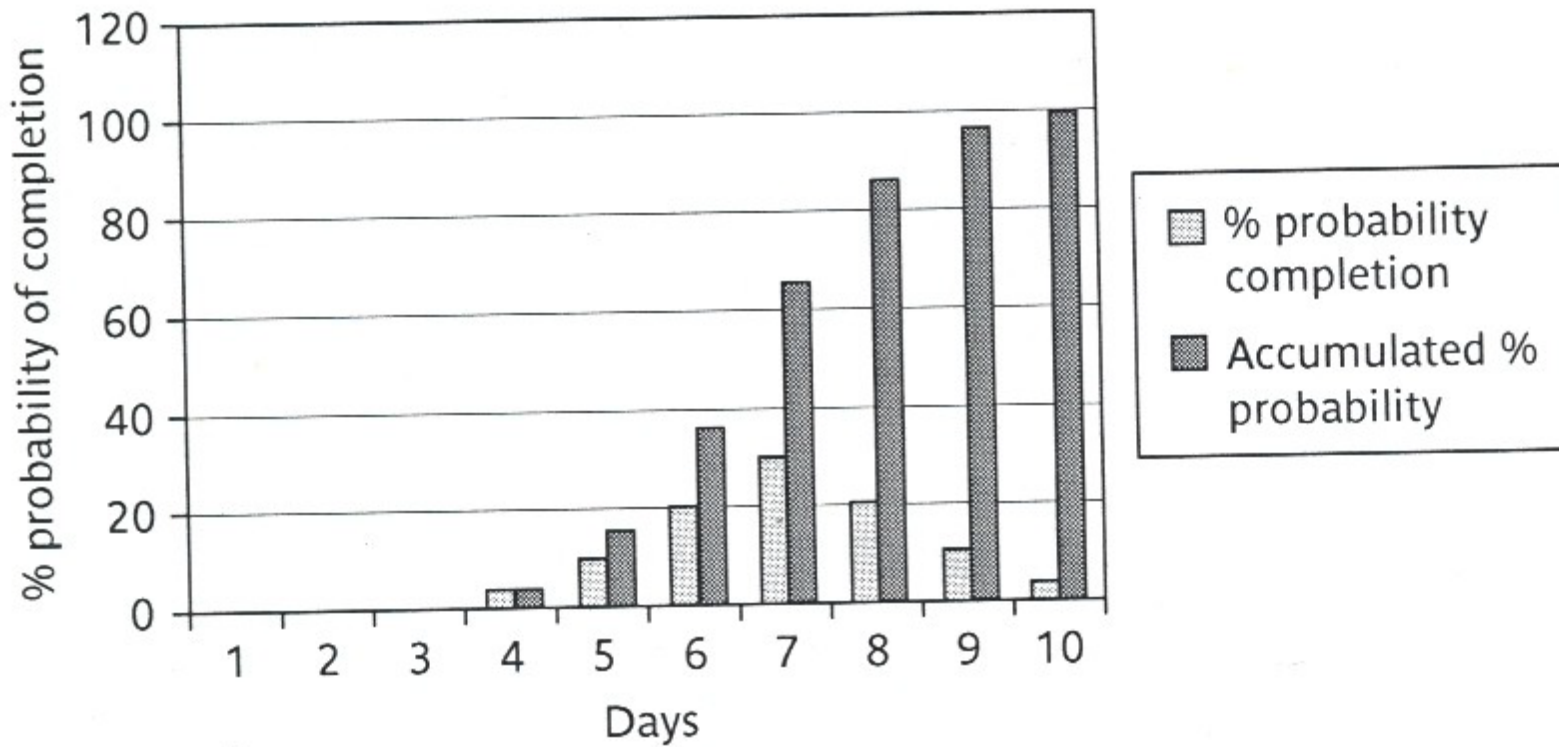
Instead of damages, there could be gains.

Example:

a task that is scheduled to take six days is completed in 3 days instead.

A project leader may produce a **probability chart for the tasks.**

Probability chart

Probability chart

● The probability completion: shows the probability of completing the task in x days.

● The accumulated probability: shows the probability of completing the task on or before the xth day.

Risk Assessment (cont'd)

2. Relative scales from 0 to 10.

- Both risk loss (damage) and the likelihood (probability of occurrence) will be assessed using relative scales from 0 to 10.

- Then they will be multiplied together to get a notional risk exposure (RE).

Risk Exposure (RE)

Ref	Hazard	Likelihood	Impact	Risk
R1	Changes to requirements specification during coding	8	8	64
R2	Specification takes longer than expected	3	7	21
R3	Significant staff sickness affecting critical path activities	5	7	35
R4	Significant staff sickness affecting non-critical activities	10	3	30
R5	Module coding takes longer than expected	4	5	20
R6	Module testing demonstrates errors or deficiencies in design	4	8	32

Risk in the table refers to the Risk Exposure (RE)

Risk Planning

- **After:**
  - The major risks are identified and
  - Prioritized.
- The task becomes "**how to deal with them**".
- **The choices for dealing with them are:**
  - Risk acceptance.
  - Risk avoidance.
  - Risk reduction and mitigation.
  - Risk transfer.

Risk Planning (cont'd)

- **Risk Acceptance:**

– This is deciding to do nothing about the risk. This means you will accept its consequences. Why?

– In order to concentrate on the more likely or damaging risks.

– The damage that those risks could cause would be less than the costs needed to act towards reducing their probability of occurrence.

Risk Planning (cont'd)

- **Risk Avoidance:**

  – Some activities are so prone to accident that it is best to avoid them altogether.

  – Example to avoid all the problems associated with developing software solutions from scratch, a solution could be to:

- Buy an off-the-shelf product.

Risk Planning (cont'd)

- **Risk Reduction and Mitigation:**

– **Risk Reduction:** attempts to reduce the <u>likelihood</u> of the risk occurring.

e.g. **consider the following risk:** developers leaving a company in the middle of a project for a better paid job.

In order to reduce the probability of such a risk occurring:

the developers could be promised to be paid generous bonuses on successful completion of the project.

Risk Planning (cont'd)

– **Risk Mitigation:** is the action taken to ensure that the <u>impact</u> of the risk is reduced when it occurs.

Taking regular backups of data storage, is it a risk mitigation measure or a risk reduction measure?

Since it would reduce the <u>impact</u> of data corruption not its <u>likelihood</u> of happening, in this sense it is <u>a data mitigation</u> measure.

Risk Planning (cont'd)

- **Risk Transfer:**
- In this case the risk is transferred to another person or organization.
- **Example:** a software development task is outsourced for a fixed fee.
- Another example is when you buy insurance(e.g. for a car).

Risk Management

Contingency Plans:

- Although risk reduction measures try to reduce the probability or the likelihood of risks, they still could happen.

- **Contingency plan** is a planned action to be carried out if a risk materializes (occurs).

Risk Management (cont'd)

Creating and maintaining the risk register:

- **A risk register:** it contains the findings of project planners of what appear to be the most threatening risks to the project.

- After work starts on a project more risks will appear and will be added to the register.

- Risk registers are reviewed and updated regularly.