Université Concordia University

SOEN – 6841
Software Project Management

Amin Ranj Bar

Winter, 2021

Overview

- Notion of Risk in Software Engineering
- Risk Management process
- Project Communication Flows

Notion of Risk in Software Engineering. ISO/IEC Definitions

- **risk:** The combination of the probability of an event and its negative consequence.

  1—The term “risk” is generally used only when there is at least the possibility of negative consequences.

  2—In some situations, risk arises from the possibility of deviation from the expected outcome or event.

- **risk category**: A class or type of risk (e.g., technical, legal, organizational, safety, economic, engineering cost, schedule).

  NOTE—A risk category is a characterization of a source of risk.

Notion of Risk in Software Engineering. SWEBOK: 2.5. Risk Management

- Risk identification and analysis (what can go wrong, how and why, and what are the likely consequences)
- Critical risk assessment (which are the most significant risks)
- Risk mitigation and contingency planning (formulating a strategy to deal with risks and to manage the risk profile)

- http://swebokwiki.org/Chapter_7:_Software_Engineering_Management

Risk Management process

- **Steps:**

1. Risk assessment
2. Risk control

- Risk assessment and risk control work together!

Risk assessment

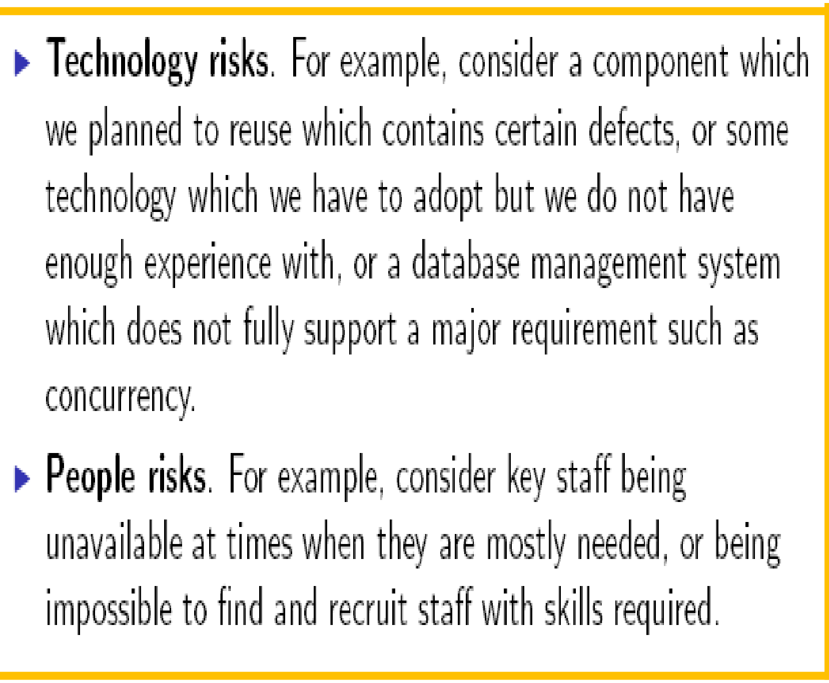
1. Risk Identification
2. Risk analysis
3. Risk prioritization

Can be performed at the beginning of the project development and reassessed at the beginning of the iterations

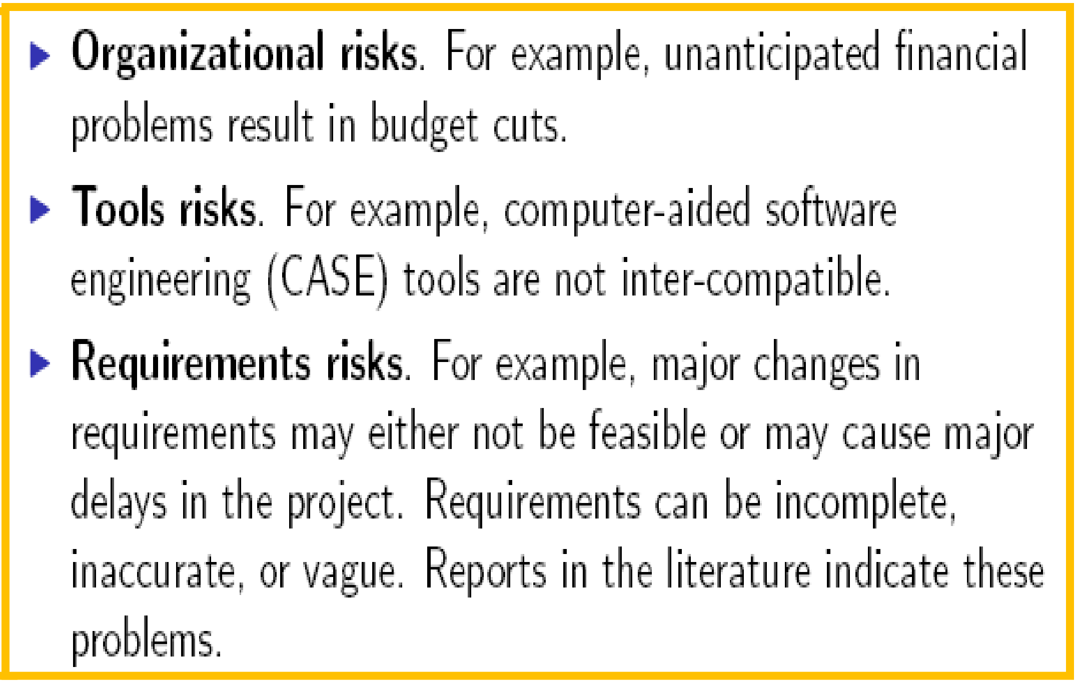
Risk control

- Risk planning
  - Can be performed at the beginning of the project development and reassessed at the beginning of the iterations
- Resolution
  - The assignment of a risk item to a person/ date by which it has to be resolved.
  - Can be performed throughout the project development
- Risk monitoring
  - Can be performed throughout the project development

Risk Categories



- **Technology risks.** For example, consider a component which we planned to reuse which contains certain defects, or some technology which we have to adopt but we do not have enough experience with, or a database management system which does not fully support a major requirement such as concurrency.
- **People risks.** For example, consider key staff being unavailable at times when they are mostly needed, or being impossible to find and recruit staff with skills required.



- **Organizational risks.** For example, unanticipated financial problems result in budget cuts.
- **Tools risks.** For example, computer-aided software engineering (CASE) tools are not inter-compatible.
- **Requirements risks.** For example, major changes in requirements may either not be feasible or may cause major delays in the project. Requirements can be incomplete, inaccurate, or vague. Reports in the literature indicate these problems.

Estimation risks. For example, the time required to complete the project has been underestimated.

Risk assessment: **Risk identification**

- Risk identification: Identify risks related to the overall project, to the product and to the business.
- The outcome of this step is a collection of risk items.
- Example:
  - You are a project manager and have been assigned to a high-profile, mission-critical project that has high-revenue potential in a new market segment.
  - After an initial assessment, you have determined that it is a risky project since it relies heavily on new technology

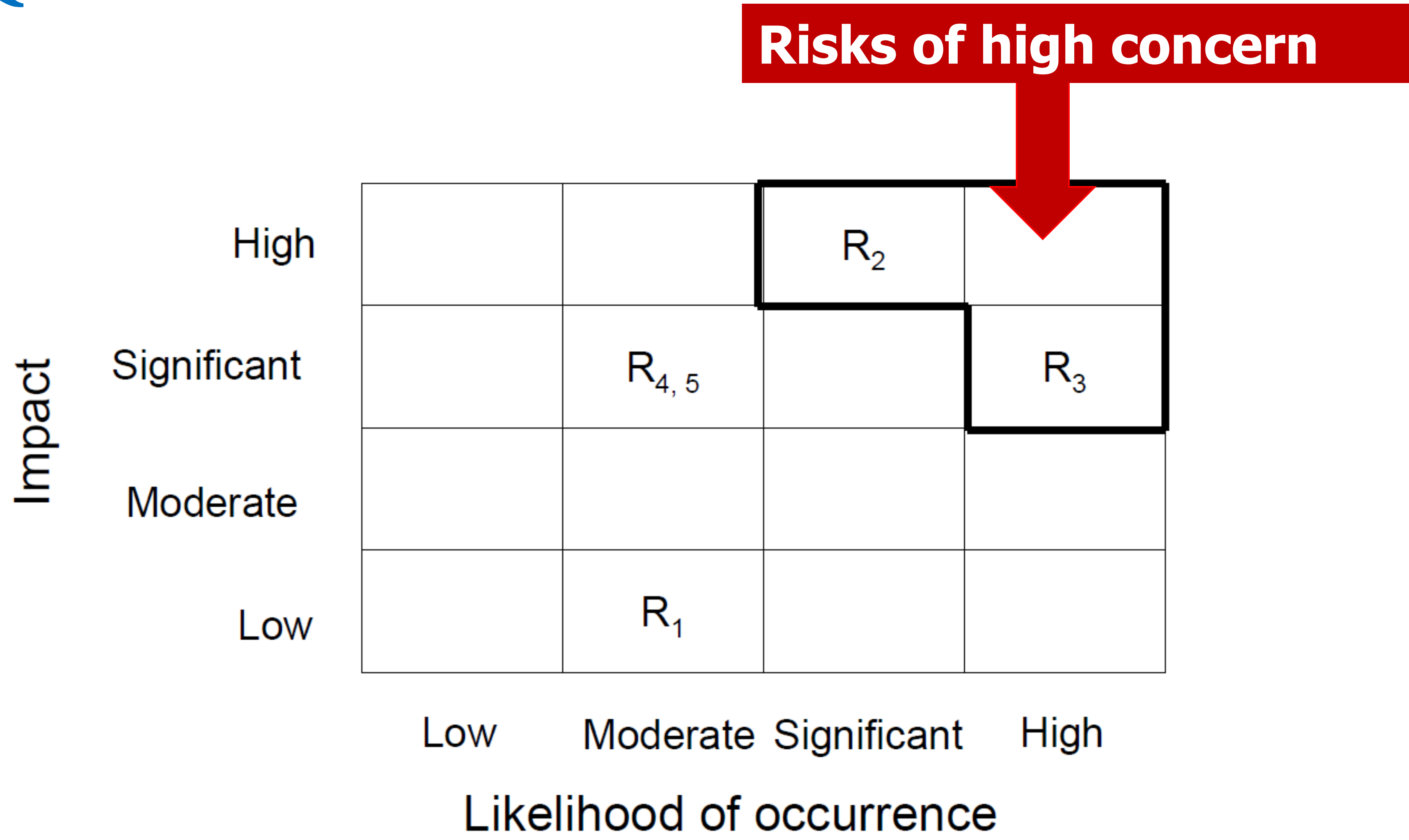
Five always-risky activities!

1. Integration
2. Data migration
3. Customization
4. Unproven technology / unproven team
5. Too-large projects

Risk assessment:
Risk analysis

- Assess:
  - the likelihood of occurrence
    - **Qualitative: Scale** (for example: **Low, Moderate, Significant, High**)
    - **Quantitative: probability of occurrence**
  - the impact on project, product and business of each risk item
    - **Qualitative: Scale** (for example: **Low, Moderate, Significant, High**)
    - **Quantitative:** where data is available.
      - *Example: fire can cause* ***0.5 millions*** *of damage in a facility*
- Which risks do we consider really serious?

Impact v.s. Likelihood of Occurrence: **Qualitative** assessment

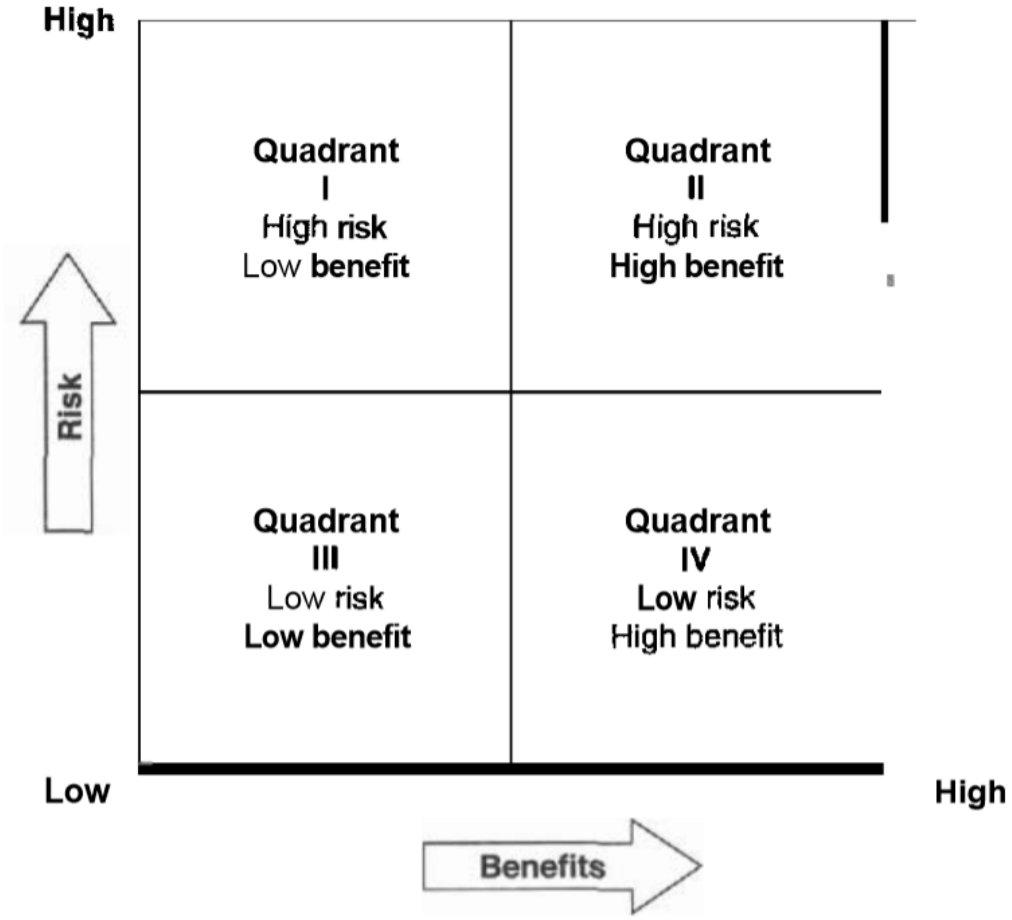


Risks of high concern

Impact	Low	Moderate	Significant	High
High			R_2	
Significant		$R_{4, 5}$		R_3
Moderate				
Low		R_1		

Likelihood of occurrence

Risk/Benefits: tradeoffs



High

Risk

Low

High

Benefits

Quadrant
I
High risk
Low **benefit**

Quadrant
II
High risk
High benefit

Quadrant
III
Low risk
Low benefit

Quadrant
IV
Low risk
High benefit

Risk/Benefits: tradeoffs

- **High risk, low benefit:** Projects are not worth doing simply because there is uncertainty about outcomes and little foreseeable payoff.
- **High risk ,high benefit:** the outcomes could substantially improve market share and profitability.
  - Example: investment in the field of space exploration.
- **Low risk, low benefit:** Projects are not worth doing because there is no foreseeable payoff.
- **Low risk, high benefit:** Projects are very attractive.
  - Example: installation of proven technology that promises to double productivity

Impact v.s. Likelihood of Occurrence: **Quantitative** assessment

Risk Exposure (RE) =

Risk-Probability * Risk-impact

Example:

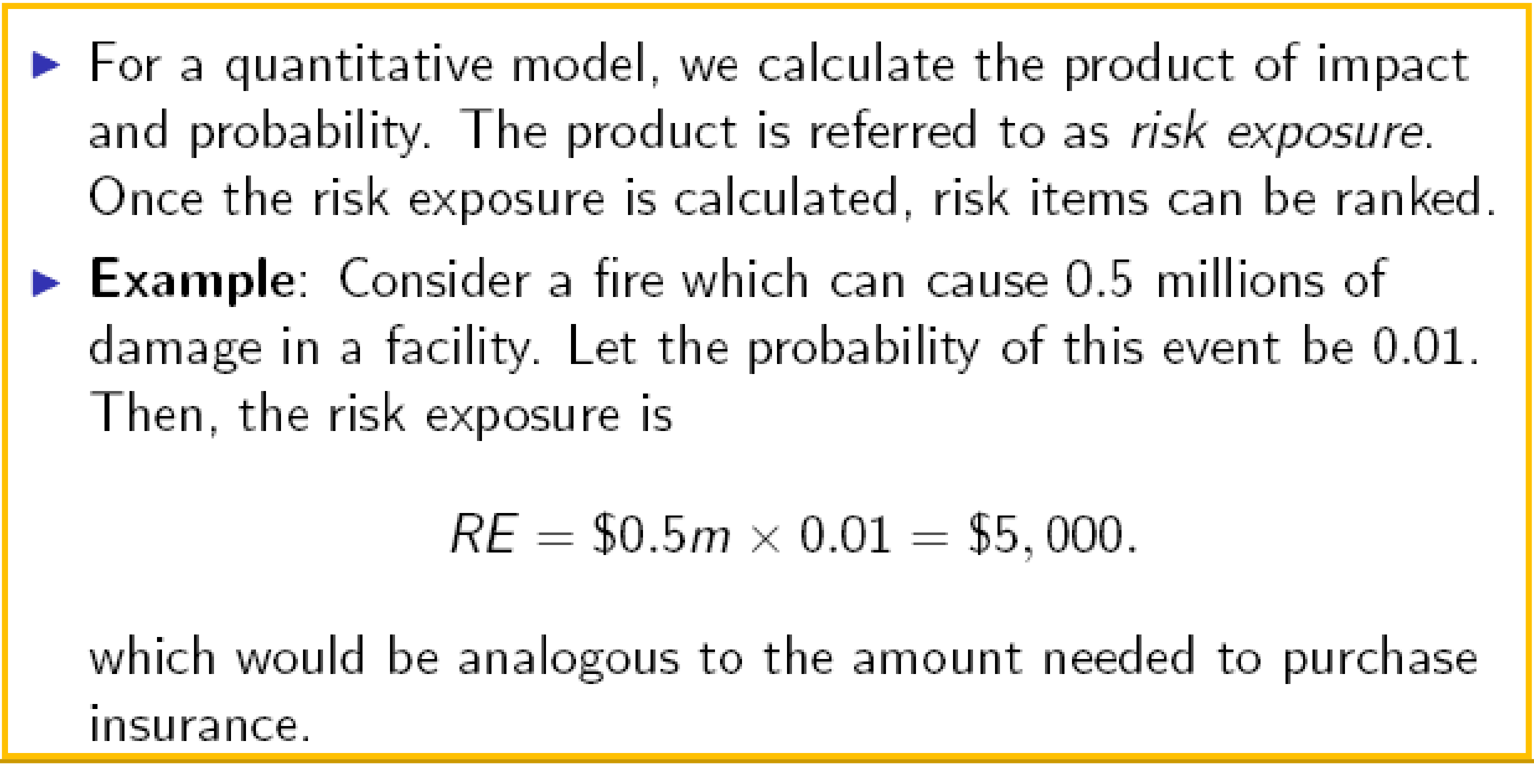
Loss of car: risk-impact is cost to replace car, e.g. $10,000

- Probability of car loss: 0.10
- Risk exposure or expected loss =
  10,000 x 0.10 = 1,000

- **Risk prioritization**: Ranking of risk items can be done based on the RE

Quantitative model: example

Risk exposure =
risk probability x impact

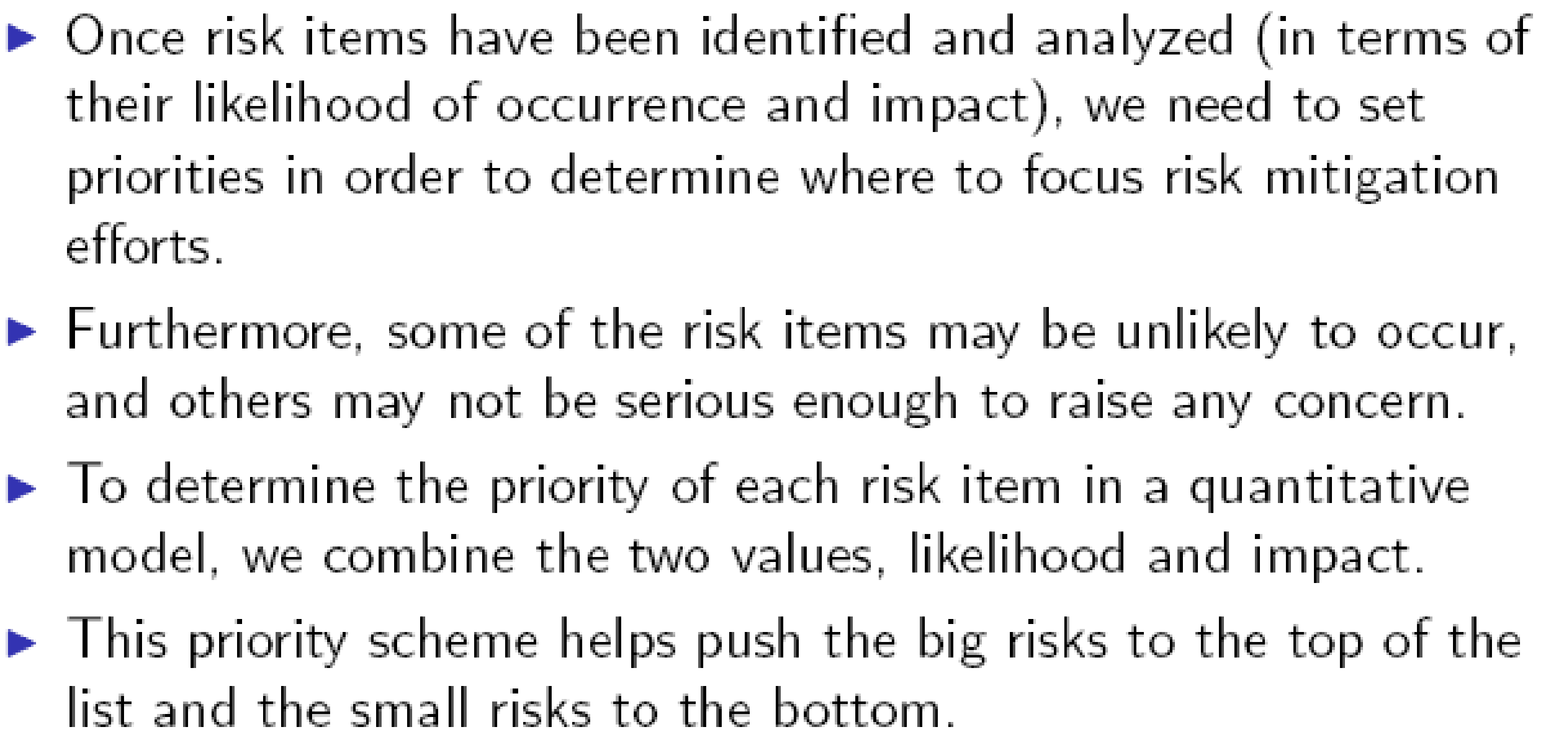


- For a quantitative model, we calculate the product of impact and probability. The product is referred to as *risk exposure*. Once the risk exposure is calculated, risk items can be ranked.
- **Example**: Consider a fire which can cause 0.5 millions of damage in a facility. Let the probability of this event be 0.01. Then, the risk exposure is

$$RE = \$0.5m \times 0.01 = \$5,000.$$

which would be analogous to the amount needed to purchase insurance.

Risk assessment:
Risk prioritization



- Once risk items have been identified and analyzed (in terms of their likelihood of occurrence and impact), we need to set priorities in order to determine where to focus risk mitigation efforts.
- Furthermore, some of the risk items may be unlikely to occur, and others may not be serious enough to raise any concern.
- To determine the priority of each risk item in a quantitative model, we combine the two values, likelihood and impact.
- This priority scheme helps push the big risks to the top of the list and the small risks to the bottom.

Risk control

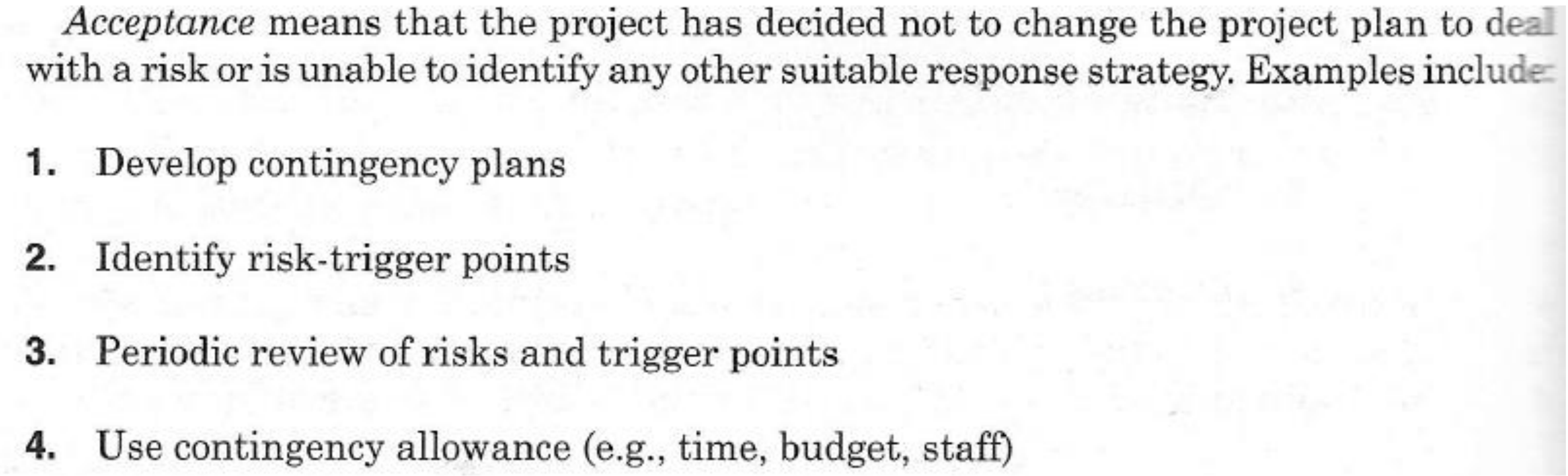
- Risk planning
  - Can be performed at the beginning of the project development and reassessed at the beginning of the iterations
- Risk Resolution
  - The assignment of a risk item to a person/ date by which it has to be resolved.
  - Can be performed throughout the project development
- Risk monitoring
  - Can be performed throughout the project development

Risk Control:

Risk planning

- Consider each risk item and develop a strategy to manage it
- Types of strategies:
  - Acceptance
  - Avoidance
  - Risk transfer
  - Mitigation
- Contingency measures

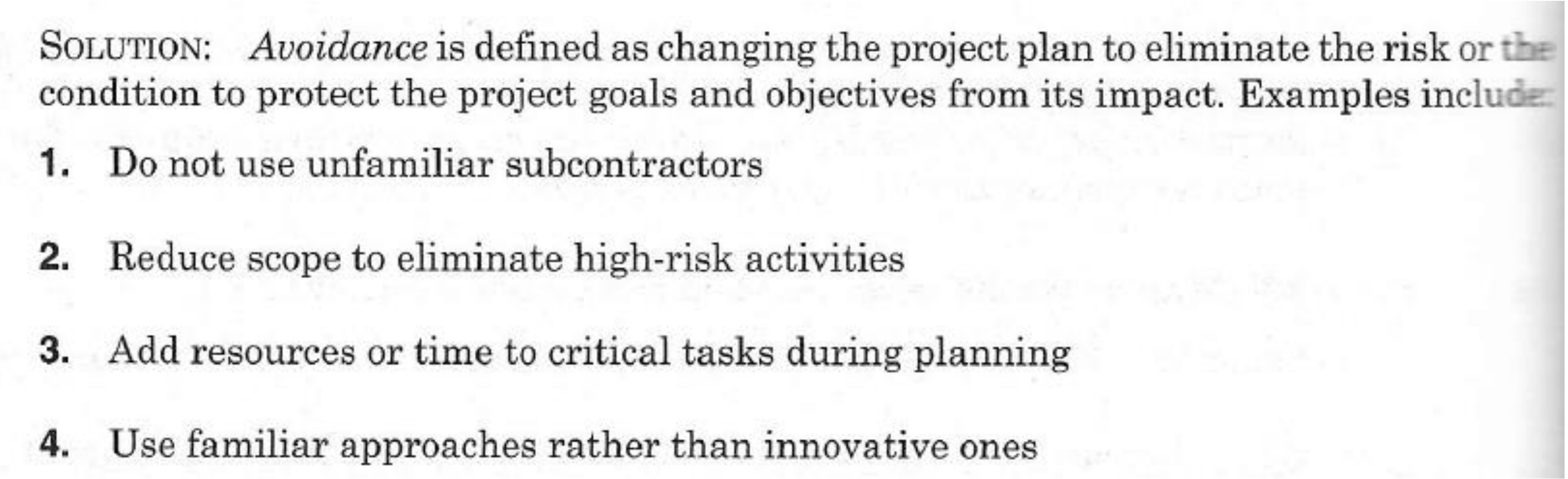
Risk response strategies: Acceptance



Acceptance means that the project has decided not to change the project plan to deal with a risk or is unable to identify any other suitable response strategy. Examples include

1. Develop contingency plans
2. Identify risk-trigger points
3. Periodic review of risks and trigger points
4. Use contingency allowance (e.g., time, budget, staff)

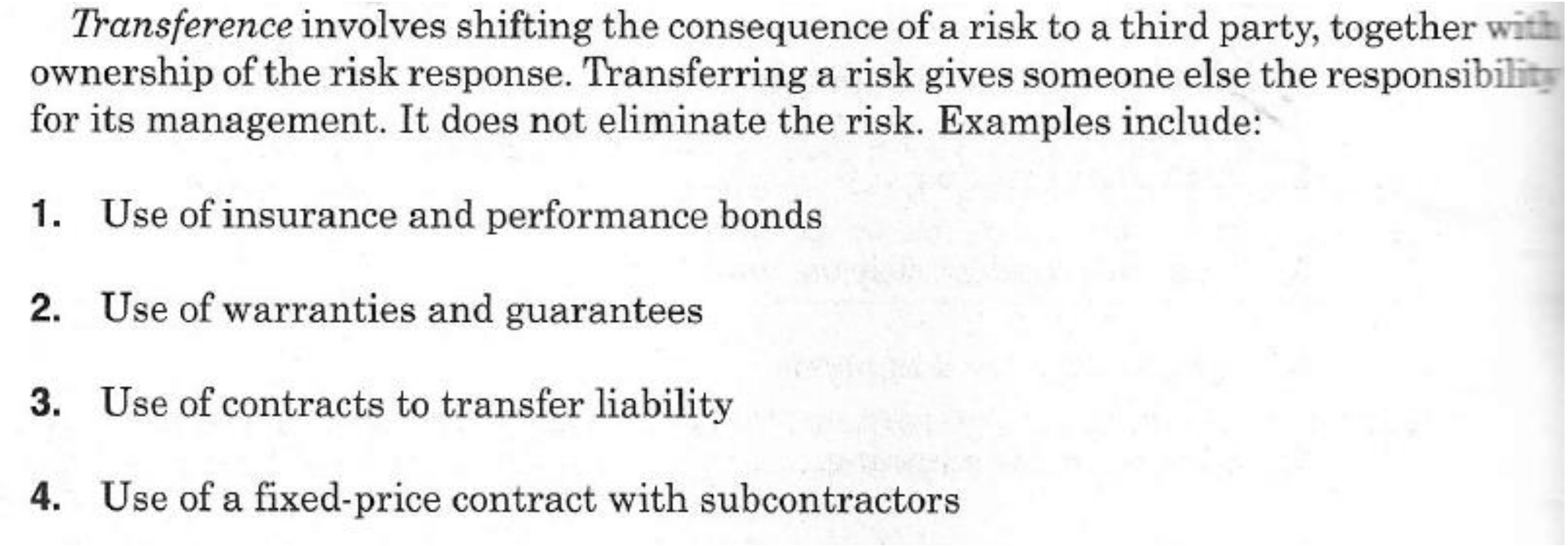
Risk response strategies: Avoidance



SOLUTION: *Avoidance* is defined as changing the project plan to eliminate the risk or the condition to protect the project goals and objectives from its impact. Examples include:

1. Do not use unfamiliar subcontractors
2. Reduce scope to eliminate high-risk activities
3. Add resources or time to critical tasks during planning
4. Use familiar approaches rather than innovative ones

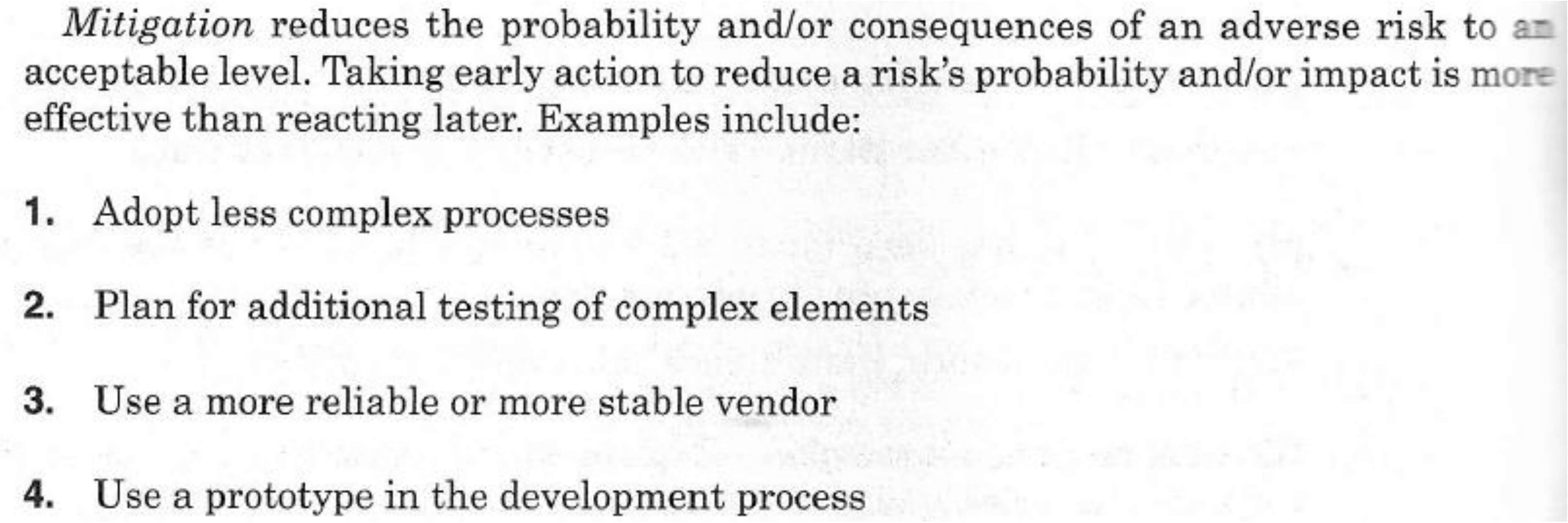
Risk response strategies: Transference



Transference involves shifting the consequence of a risk to a third party, together with ownership of the risk response. Transferring a risk gives someone else the responsibility for its management. It does not eliminate the risk. Examples include:

1. Use of insurance and performance bonds
2. Use of warranties and guarantees
3. Use of contracts to transfer liability
4. Use of a fixed-price contract with subcontractors

Risk response strategies: Mitigation



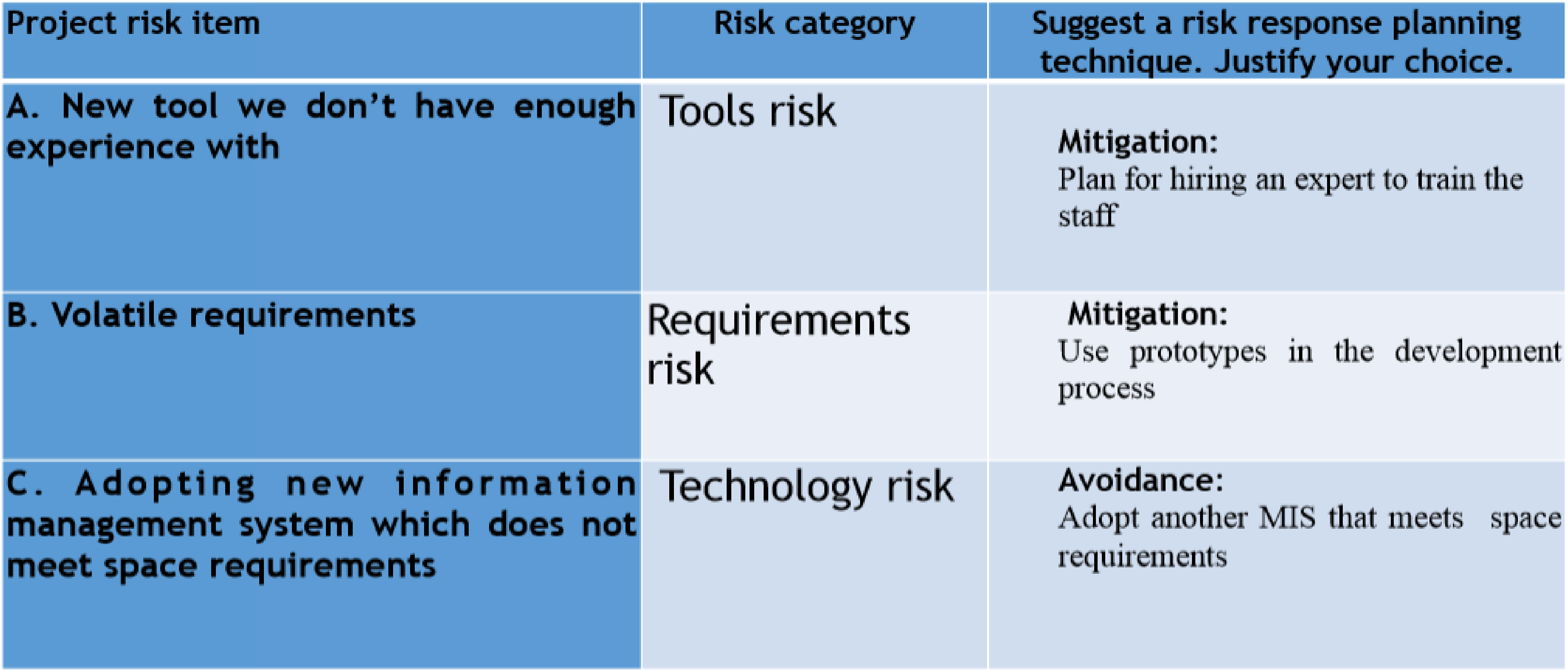
Mitigation reduces the probability and/or consequences of an adverse risk to an acceptable level. Taking early action to reduce a risk's probability and/or impact is more effective than reacting later. Examples include:

1. Adopt less complex processes
2. Plan for additional testing of complex elements
3. Use a more reliable or more stable vendor
4. Use a prototype in the development process

Exercise: Risk identification & Risk response strategies:

Project risk item	Risk category	Suggest a risk response planning technique. Justify your choice.
A. New tool we don’t have enough experience with		
B. Volatile requirements		
C. Adopting new information management system which does not meet space requirements		

solution



Project risk item	Risk category	Suggest a risk response planning technique. Justify your choice.
A. New tool we don’t have enough experience with	Tools risk	**Mitigation:** Plan for hiring an expert to train the staff
B. Volatile requirements	Requirements risk	**Mitigation:** Use prototypes in the development process
C. Adopting new information management system which does not meet space requirements	Technology risk	**Avoidance:** Adopt another MIS that meets space requirements

Risk response strategies: Mitigation

- We can take measures to reduce the risk exposure factor of a given risk item.
- However, we need to take into consideration that these measures contain cost:

Risk Reduction Leverage =

((risk exp. RE before) – (risk exp. RE after)) / (cost of reduction)

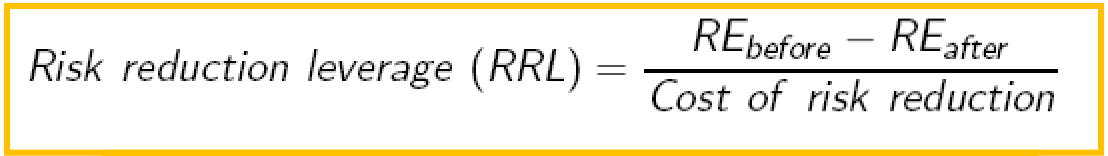
Risk reduction leverage (RRL)

- We define *risk reduction leverage* as the ratio of the reduction in risk exposure over the cost of the reduction (countermeasure).

$$Risk\ \ reduction\ \ leverage\ (RRL) = \frac{RE_{before} - RE_{after}}{Cost\ \ of\ \ risk\ \ reduction}$$

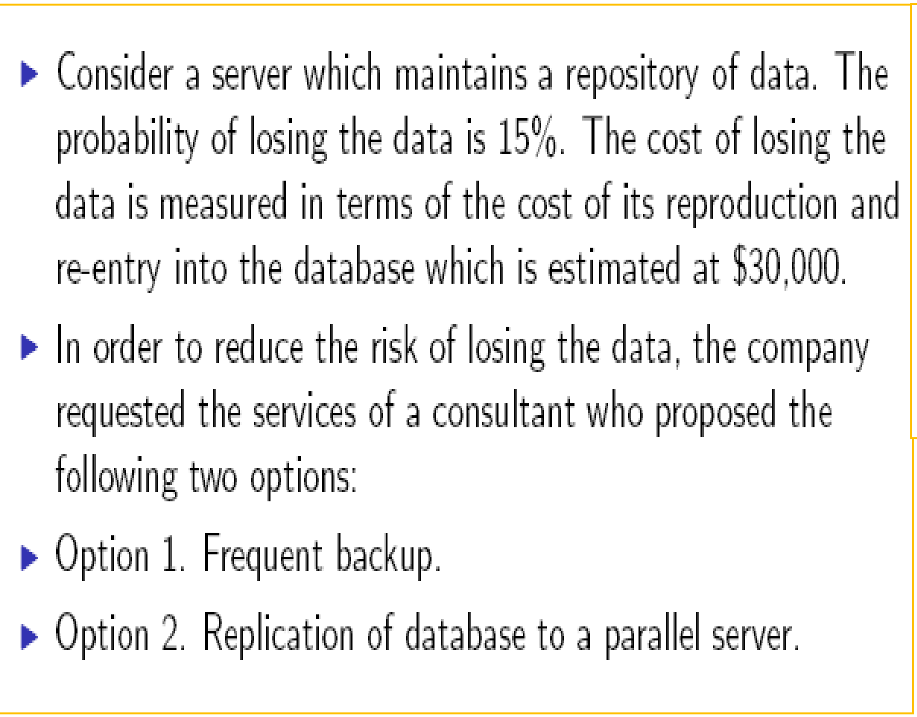
  - According to the definition, values of *RRL* greater than 1 indicate cost effective risk reduction measures because the reduction in risk exposure achieved by taking some measure is greater than the costs involved.
  - On the other hand, values of *RRL* less than 1 would indicate non cost effective measures.

Risk reduction leverage (RRL) exercise

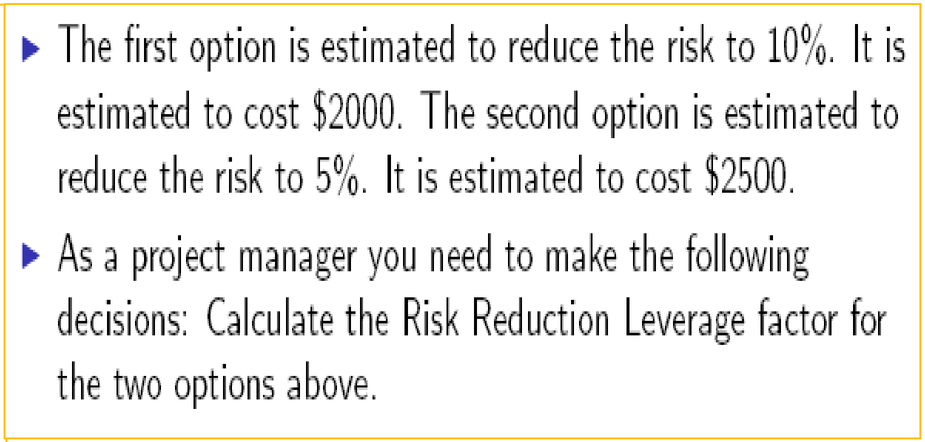


$$\textit{Risk reduction leverage (RRL)} = \frac{RE_{before} - RE_{after}}{\textit{Cost of risk reduction}}$$

RE = risk probability x amount at stake



- Consider a server which maintains a repository of data. The probability of losing the data is 15%. The cost of losing the data is measured in terms of the cost of its reproduction and re-entry into the database which is estimated at $30,000.
- In order to reduce the risk of losing the data, the company requested the services of a consultant who proposed the following two options:
- Option 1. Frequent backup.
- Option 2. Replication of database to a parallel server.

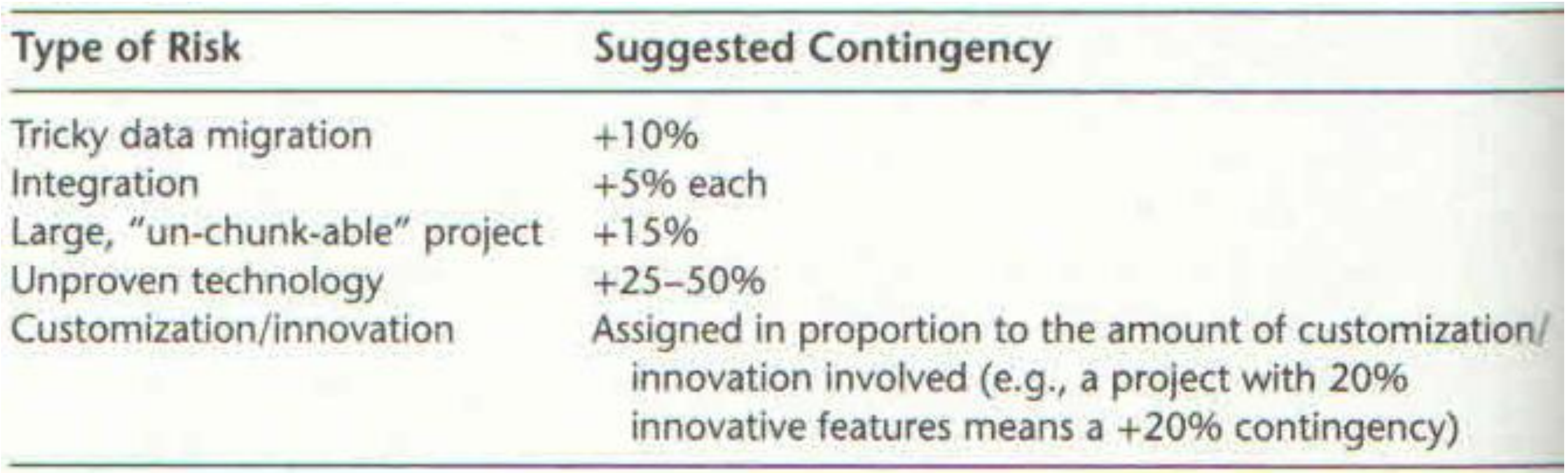


- The first option is estimated to reduce the risk to 10%. It is estimated to cost $2000. The second option is estimated to reduce the risk to 5%. It is estimated to cost $2500.
- As a project manager you need to make the following decisions: Calculate the Risk Reduction Leverage factor for the two options above.

Which option would you adopt, if any?

Finish up budgeting:
The Cost of Consequences

- Identify the risks you are accepting and mitigating
- For the purposes of budgeting, assign a percentage to each risk
- Example:



Type of Risk	Suggested Contingency
Tricky data migration	+10%
Integration	+5% each
Large, "un-chunk-able" project	+15%
Unproven technology	+25–50%
Customization/innovation	Assigned in proportion to the amount of customization/ innovation involved (e.g., a project with 20% innovative features means a +20% contingency)

Finish up budgeting: Contingency Percentage Factors (assigning $$-value to risk)

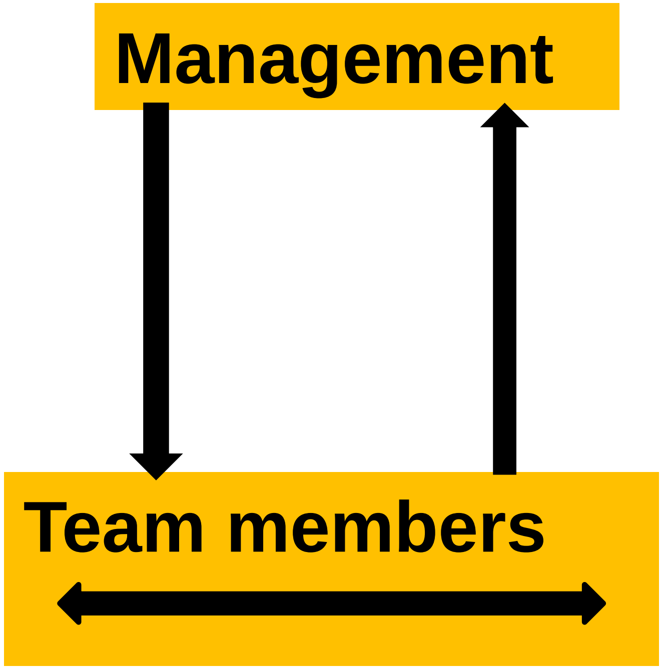
- Rule of thumb to calculate contingency (see the example below)

Budget	**$250,000**
Large project factor	$37,500
Integration factor	$25,000
Innovation factor	$12,500
Total contingency	*$75,000*
Total budget	**$325,000**

Risk monitoring & Controlling

- Project risk response audits
  - Examining and documenting the effectiveness of risk responses in dealing with identified risks, their root causes, and the risk management process
  - PM should make sure it is done regularly
  - Should have clear format and objectives
- Periodic project risk reviews
  - Identification of new risks
  - Reassessment of current risks
  - Closing outdated risks
- Additional risk response planning

Project Communication Flows: down, up and across



Management

Team members

Monthly Steering Committee

- Attendees
- Agenda:
  - Reporting on timeline
  - Reporting on budget
  - Key accomplishments in preceding month
  - Plan for upcoming month
  - Problems, discoveries (such as budget shift, consumption of contingency, large new feature) that require committee’s agreement

Weekly Project Management Meeting

- Attendees
- Agenda
  - Reporting on all tracks of the project with discussion and problem solving as appropriate
  - Identifying to-does and follow-ups
  - Tasks in the upcoming week

Daily Standup Meeting

- 15 min
- Team members report on what they are working on, their progress, barriers to their work, in any.

Well-run meetings

- Agenda
- Insist on attention
- timeliness
- Follow-up notes

Summary

- Notion of Risk in Software Engineering
- Risk Management process
- Project Communication Flows