

# Foundations of Project Management

**PMG 101**  
**Managing Risk**

## Chapter 8



## Managing Risk

Risk Management Process

Step 1: Risk Identification

Step 2: Risk Assessment

Step 3: Risk Response Development

Opportunity Management

Contingency Planning

Contingency Funding and Time Buffers

Step 4: Risk Response Control

Change Control Management

- Learning objectives

# How risk averse are you?

**Risk averse people:**

- ☐ I like being dependable and I'm usually punctual.
- ☐ I am not likely to take chances.
- ☐ I am responsible and prefer to work efficiently.
- ☐ I am more service oriented than self oriented.
- ☐ I value institutions and observe traditions

**Risk seeking people:**

- ☐ I like action, and I act impulsively at times.
- ☐ I seek excitement for the thrill of the experience.
- ☐ I am resourceful and prefer not to plan or prepare.
- ☐ I am more self oriented than service oriented.
- ☐ I like to anticipate another person's position.

**Risk neutral people:**

- ☐ I trust my intuition, and I am comfortable with unknown.
- ☐ I think about the future and have long-range objectives.
- ☐ I am naturally curious and often ask, "Why?"
- ☐ I enjoy generating new ideas.
- ☐ I work best when I am inspired.

# Black Swans

They are unpredictable or unforeseen event, typically one with extreme consequences.

Risk management: There are no black swans

- The March 2011 earthquake and tsunami and crisis with the nuclear plant.
  - Could not happen
  - Sea walls were tall enough
    - Historical record says otherwise
  - Generators were ready
    - Assuming no tsunami could hit
- BP Oil spill in April 2010
  - Blow out preventer would work
    - Known problems
  - Management was on top of the problems
  - “Excellent record of safety”.

# What can Possibly Go Wrong?

Consider the “average” college student:

- What risks does the student encounter? How can we mitigate the damage?
  - Computer related:
    - » Lose file;
    - » Lose flash drive;
    - » Lose hard drive; damaged
    - » Lose computer; damaged, lost or stolen
    - » Crash computer; corrupted files
    - » No network? Cannot access D2L
  - Attendance and time management
    - » Miss class or late
    - » Late home work submission
    - » Miss home work submission

# What can Possibly Go Wrong?

Consider the “average” project:

- Testing takes longer than planned – cannot resolve bugs
- Vendor cannot deliver a product on schedule
- Critical engineer
  - Has accident (wipes out in ski jump)
  - Becomes a parent
  - Has major surgery
- Critical engineer leaves project/company
- Change of ownership. Project on hold
- Major downsizing
- Dysfunctional staff
- Blizzard and power failures

# Risk definition

- **Risk** is an uncertain event or condition that, if it occurs, has a positive or negative effect on project objectives.
- **Risk** has a cause and, if it occurs, a consequence. For example, a cause may be a flu virus or change in scope requirements. The event is that team members get stricken with the flu or the product has to be redesigned. If either of these uncertain events occurs, it will impact the cost, schedule, and /or quality of the project. Some potential risk events can be identified before the project starts—such as equipment malfunction or change in technical requirements. Risks can be anticipated consequences, like schedule slippages or cost overruns. Risks can be beyond imagination like the 2008 financial meltdown.
- While risks can have positive consequences such as unexpected price reduction in materials, the focus of this chapter is on what can go wrong (negative) and the risk management process.

# Risk definition

- “Not all risks are bad: Risks can present opportunities as well as threats to a project.
- Risk originates in the uncertainty associated with any project – remember, projects are unique

## Project Risks

- What can go wrong?
- What is the likelihood?
- What will the damage be?
- What can we do about it?

# How to Categorize Risk

## Risks: known, unknown, unknowable

- **Known Risks:** Risks that can be uncovered after careful evaluation of the project plan, business and technical environment, and other reliable sources of information (I.e. unrealistic delivery dates, lack of user input, etc.)
  - Refer to those risks that can **be estimated** from historical information
  - Can be mitigated by management techniques and through response plans, should they occur
  - *Example:* Potential delay in delivery from third-party vendor

# How to Categorize Risk

- **Predictable Risks** [but **unknown** risks]: Risks that can be extrapolated from past projects. (Staff turnover, poor communication with the customer)
  - Refer to those risks that we know have a probability of occurring, but do **not know** the precise impact
  - Cannot be managed directly but can be mitigated by the use of contingency
  - *Example:* Loss of key personnel due to turnover
- **Unpredictable Risks**  
“Joker” risks that are hard to predict.
- **Unknowable risks**
  - Refer to those risks that are outside the scope of historical or probabilistic models for the project
  - Are beyond the scope of risk management and usually are addressed by *crisis* or *disaster management*
  - *Examples:* Corporate failures, natural disasters, acts of terrorism or war, major snowstorm and power loss

## Risk management

**Risk management** attempts to recognize and manage potential and unforeseen trouble spots that may occur when the project is implemented. Risk management identifies as many risk events as possible (what can go wrong), minimizes their impact (what can be done about the event before the project begins), manages responses to those events that do materialize (contingency plans), and provides contingency funds to cover risk events that actually materialize.

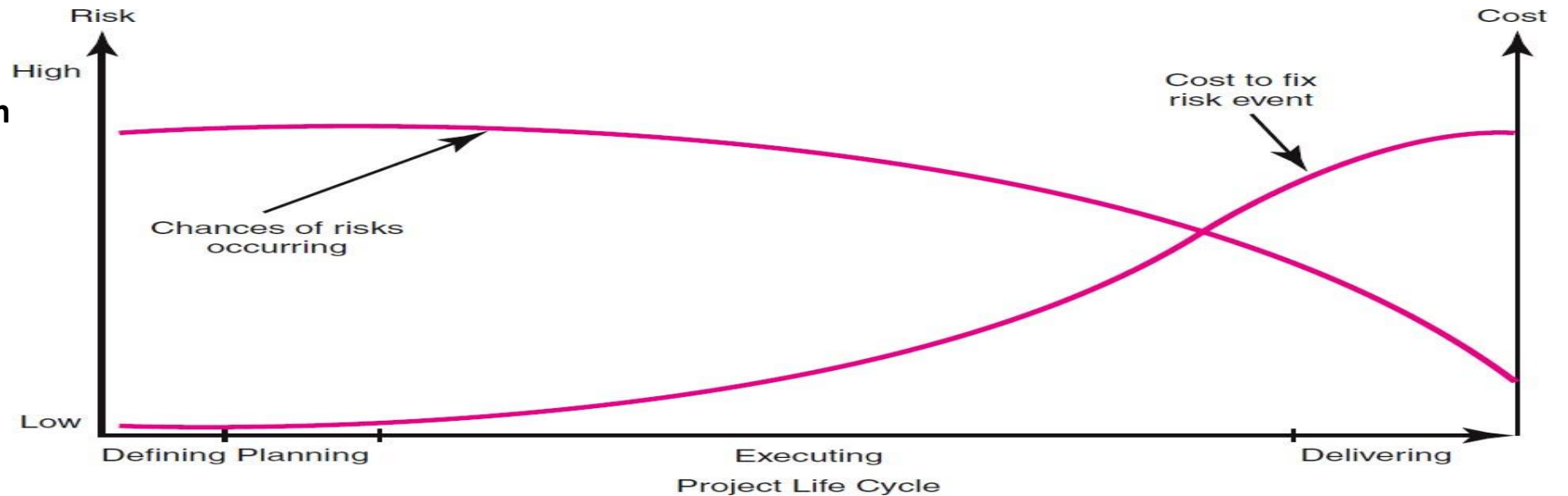
### Risk Management Process

Figure 7.1 presents a graphic model of the risk management challenge. The chances of a risk event occurring (e.g., an error in time estimates, cost estimates, or design technology) are greatest in the concept, planning, and start-up phases of the project.

- **Risk Management Process**

- For example, the risk event of a design flaw occurring after a prototype has been made has a greater cost or time impact than if the event occurred in the start-up phase of the project. Clearly, identifying project risk events and deciding a response before the project begins is a more prudent approach than not attempting to manage risk.

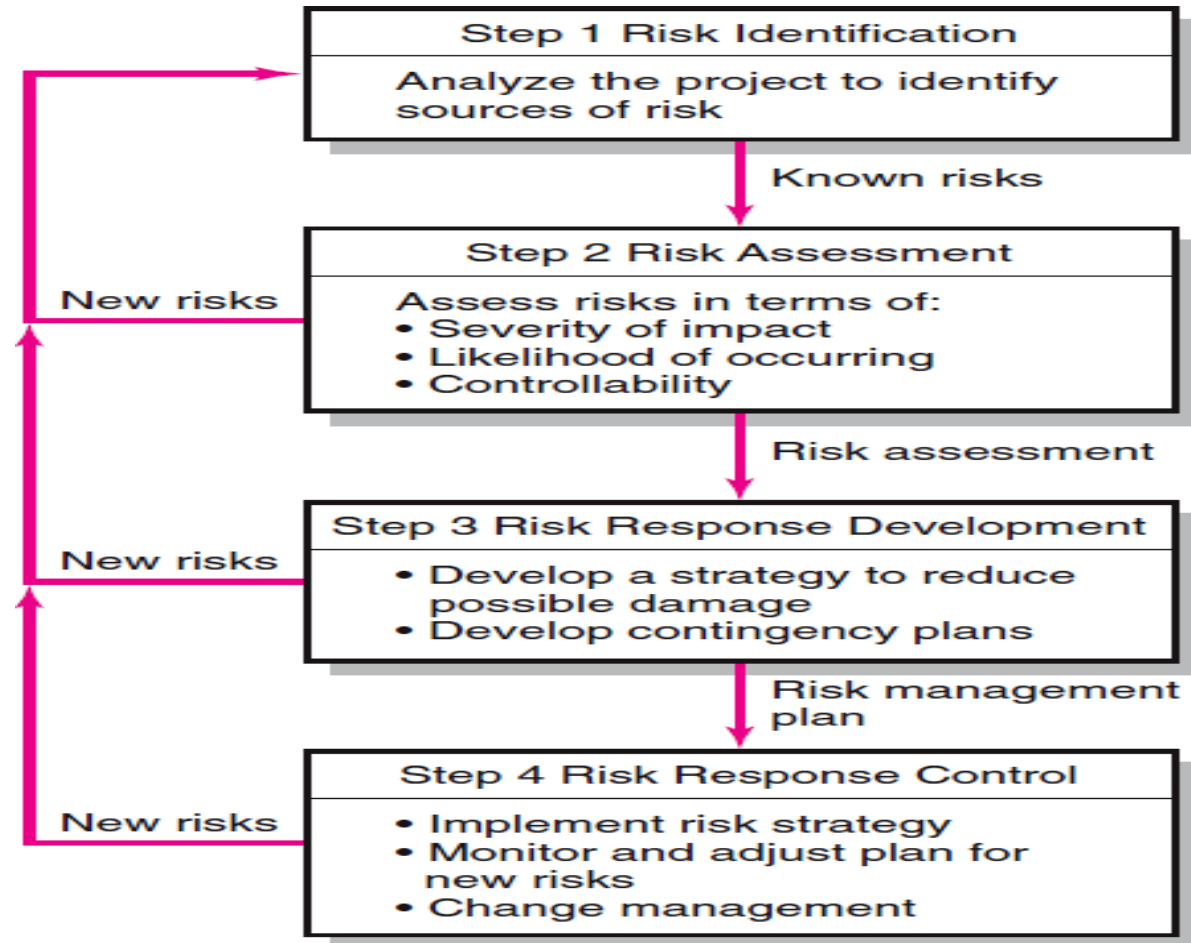
- **Figure 7.1: Risk event graph**



## Risk management process

**Risk management** is a proactive approach rather than reactive. It is a preventive process designed to ensure that surprises are reduced and that negative consequences associated with undesirable events are minimized. It also prepares the project manager to take action when a time, cost, and/or technical advantage is possible.

Successful management of project risk gives the project manager better control over the future and can significantly improve chances of reaching project objectives on time, within budget, and meeting required technical (functional) performance.



**FIGURE 7.2**  
The Risk  
Management Process

FIGURE 7.2

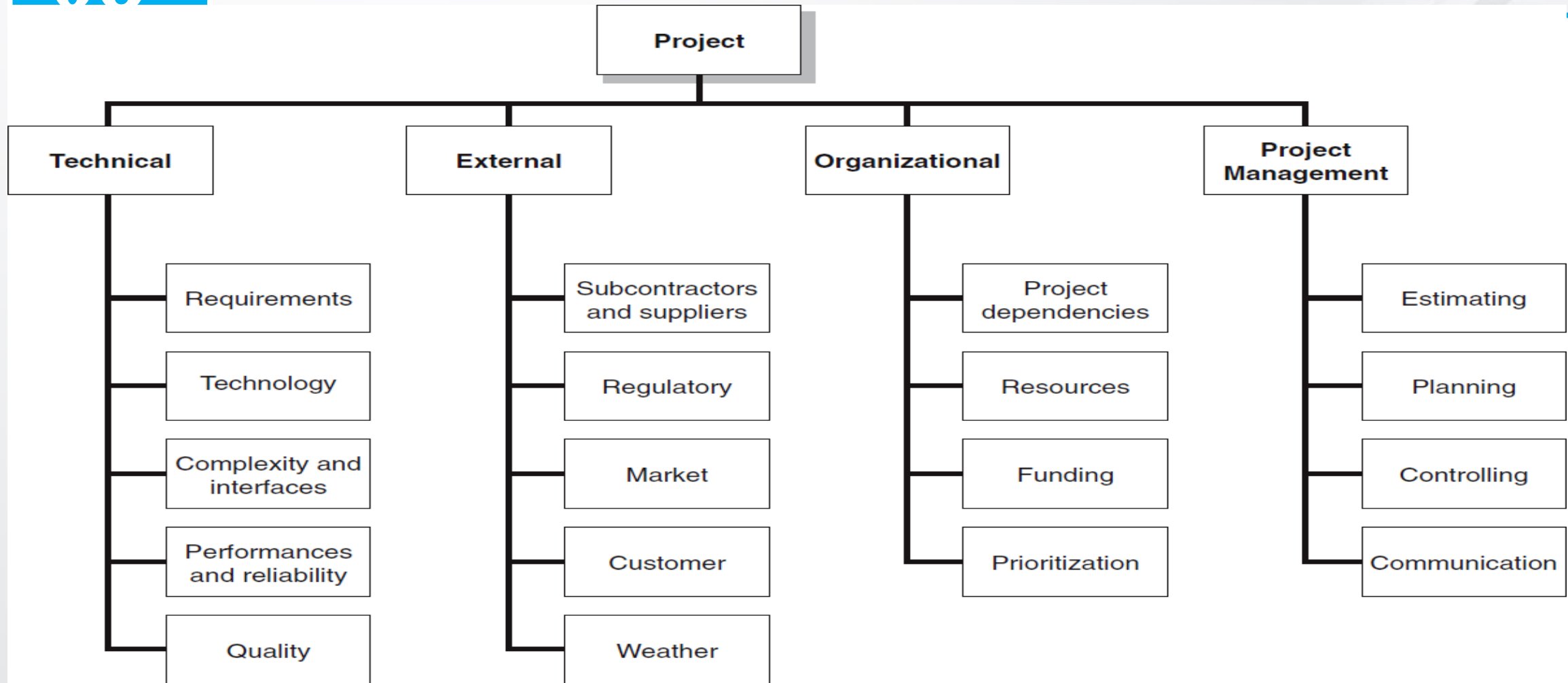
# Step 1: Risk Identification

The risk management process begins by trying to generate a list of all the possible risks that could affect the project. Typically the project manager pulls together, during the planning phase, a risk management team consisting of core team members and other relevant stakeholders. The team uses brainstorming and other problem identifying techniques to identify potential problems. Participants are encouraged to keep an open mind and generate as many probable risks as possible.

One common mistake that is made early in the risk identification process is to focus on objectives and not on the events that could produce consequences. For example, team members may identify failing to meet schedule as a major risk. What they need to focus on are the events that could cause this to happen (i.e., poor estimates, adverse weather, shipping delays, etc.). Only by focusing on actual events can potential solutions be found.

## 1- Risk breakdown structures (RBSs) :

- Organizations use risk breakdown structures (RBSs) in conjunction with work breakdown structures (WBSs) to help management teams identify and eventually analyze risks. Figure 7.3 provides a generic example of an RBS. The focus at the beginning should be on risks that can affect the whole project as opposed to a specific section of the project or network.
- After the macro risks have been identified, specific areas can be checked. An effective tool for identifying specific risks is the work breakdown structure. Use of the RBS reduces the chance a risk event will be missed. On large projects multiple risk teams are organized around specific deliverables and submit their risk management reports to the project manager.

**FIGURE 7.3** The Risk Breakdown Structure (RBS)

- Risk sources are identified during risk identification phase.
- Risk categories systematically classify risks and provide a context for understanding those risks
- Starting point list of risk categories:
  - Technical, quality, or performance risks
  - Project management risks
  - Organizational risks
  - External risks

- **Technical/quality/performance risks**

- Unproven or complex technology
- Changes to technology anticipated during the course of the project
- Unrealistic quality goals
- Unrealistic performance goals

- **Project management risks**

- Improper schedule and resource planning
- Poor project planning
- Improper or poor project management disciplines or methodologies

## ■ Organizational risks

- Resource conflicts due to multiple projects occurring at the same time in the organization
- Unrealistic scope, time, and cost objectives with respect to the organization's resources or structure
- Lack of funding for the project or diversion of funds from the project to other projects
- Management oversight changes
- Loss of project 'champion'
- Project 'politics'

## ■ External risks

- New laws or regulations
- Labor issues
- Weather
- Exchange rates
- Changes in foreign policy for projects performed (all or in part) in other countries
- Catastrophic risks (*force majeure*) are outside the scope of risk management planning – require disaster recovery techniques
  - » Examples: Earthquakes, meteorites, volcanoes, hurricanes, floods, civil unrest, terrorism, etc.

Since such external risks are usually considered before the decision to go ahead with the project, they will be excluded from the discussion of project risks. However, external risks are extremely important and must be addressed.

## 2- Risk profile:

- A risk profile is another useful tool. A risk profile is a list of questions that address traditional areas of uncertainty on a project. These questions have been developed and refined from previous, similar projects. Figure 7.4 provides a partial example of a risk profile.
- Risk profiles are generated and maintained usually by personnel from the project office. They are updated and refined during the post project audit. These profiles, when kept up to date, can be a powerful resource in the risk management process. The collective experience of the firm's past projects resides in their questions.

## FIGURE 7.4

### Partial Risk Profile for Product Development Project

#### Technical Requirements

Are the requirements stable?

#### Design

Does the design depend on unrealistic or optimistic assumptions?

#### Testing

Will testing equipment be available when needed?

#### Development

Is the development process supported by a compatible set of procedures, methods, and tools?

#### Schedule

Is the schedule dependent upon the completion of other projects?

#### Budget

How reliable are the cost estimates?

#### Quality

Are quality considerations built into the design?

#### Management

Do people know who has authority for what?

#### Work Environment

Do people work cooperatively across functional boundaries?

#### Staffing

Is staff inexperienced or understaffed?

#### Customer

Does the customer understand what it will take to complete the project?

#### Contractors

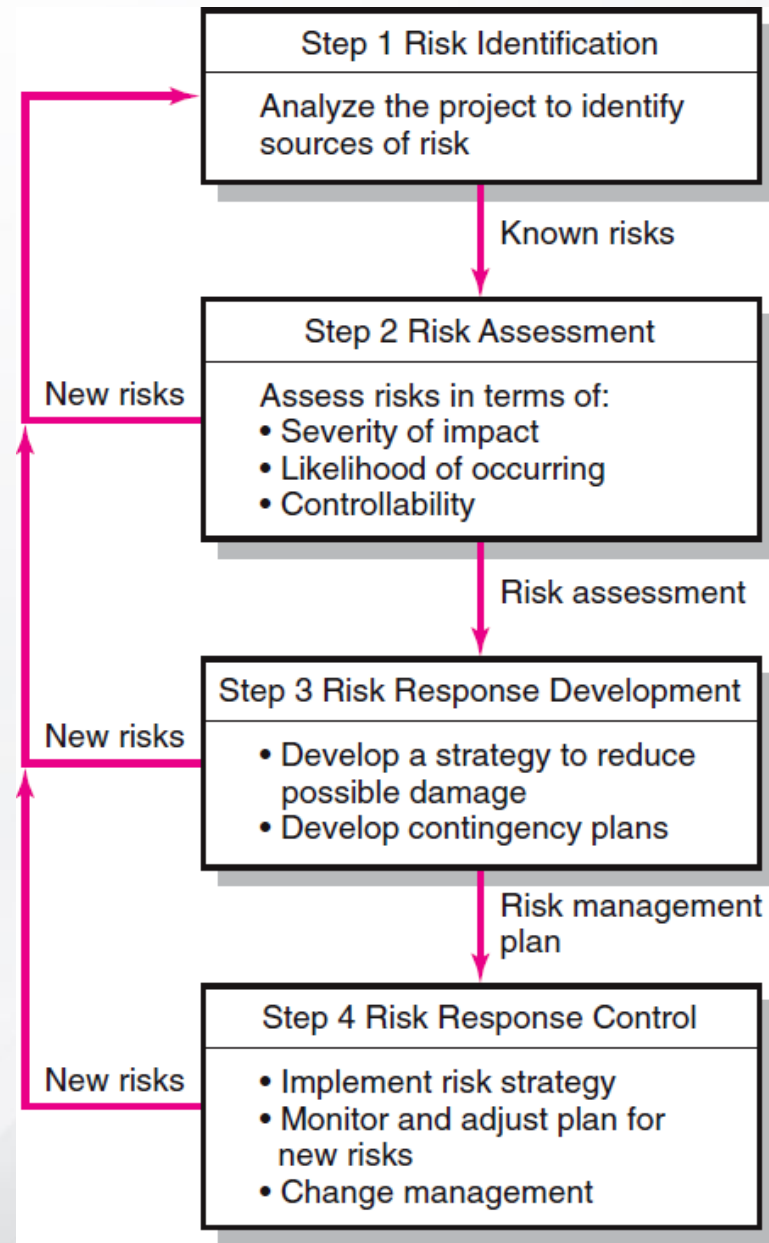
Are there any ambiguities in contractor task definitions?

FIGURE 7.4

## Risk Identification tools

### 3- Historical records:

- Historical records can complement or be used when formal risk profiles are not available. Project teams can investigate what happened on similar projects in the past to identify potential risks. For example, a project manager can check the on- time performance of selected vendors to gauge the threat of shipping delays. IT project managers can access “best practices” papers detailing other companies’ experiences converting software systems. Inquiries should not be limited to recorded data. Savvy project managers tap the wisdom of others by seeking the advice of veteran project managers.
- The risk identification process should not be limited to just the core team. Input from customers, sponsors, subcontractors, vendors, and other stakeholders should be solicited. Relevant stakeholders can be formally interviewed or included on the risk management team. Not only do these players have a valuable perspective, but by involving them in the risk management process they also become more committed to project success.



**FIGURE 7.2**  
**The Risk Management Process**

**FIGURE 7.2**

## **Step 2 Risk Assessment:**

Step 1 produces a list of potential risks. Not all of these risks deserve attention. Some are trivial and can be ignored, while others pose serious threats to the welfare of the project. Managers have to develop methods for sifting through the list of risks, eliminating inconsequential or redundant ones and stratifying worthy ones in terms of importance and need for attention.

### **Risk assessment tools**

#### **1- Scenario analysis**

It is the easiest and most commonly used technique for analyzing risks. Team members assess the significance of each risk event in terms of:

- Probability of the event.
- Impact of the event.

Simply stated, risks need to be evaluated in terms of the likelihood the event is going to occur and the impact or consequences of its occurrence.

### 1- Scenario analysis

For example, the risk of a project manager being struck by lightning صاعقة at a work site would have major negative impact on the project, but the likelihood is so low it is not worthy of consideration. Conversely, people do change jobs, so an event like the loss of key project personnel would have not only an adverse impact but also a high likelihood of occurring in some organizations. If so, then it would be wise for that organization to be proactive and mitigate this risk by developing incentive schemes for retaining specialists and/or engaging in cross-training to reduce the impact of turnover.

The quality and credibility of the risk analysis process requires that different levels of risk probabilities and impacts be defined. These definitions vary and should be tailored to the specific nature and needs of the project. For example, a relatively simple scale ranging from “very unlikely” to “almost certainly” may suffice for one project, whereas another project may use more precise numerical probabilities (e.g., 0.1, 0.3, 0.5, . . .). Figure 7.5 provides an example of how impact scales could be defined given the project objectives of cost, time, scope, and quality.

**FIGURE 7.5** Defined Conditions for Impact Scales of a Risk on Major Project Objectives (Examples for negative impacts only)

| Relative or Numerical Scale |                                       |                                               |                                             |                                           |                                         |
|-----------------------------|---------------------------------------|-----------------------------------------------|---------------------------------------------|-------------------------------------------|-----------------------------------------|
| Project Objective           | 1<br>Very Low                         | 2<br>Low                                      | 3<br>Moderate                               | 4<br>High                                 | 5<br>Very High                          |
| Cost                        | Insignificant cost increase           | < 10% cost increase                           | 10–20% cost increase                        | 20–40% cost increase                      | > 40% cost increase                     |
| Time                        | Insignificant time increase           | < 5% time increase                            | 5–10% time increase                         | 10–20% time increase                      | > 20% time increase                     |
| Scope                       | Scope decrease barely noticeable      | Minor areas of scope affected                 | Major areas of scope affected               | Scope reduction unacceptable to sponsor   | Project end item is effectively useless |
| Quality                     | Quality degradation barely noticeable | Only very demanding applications are affected | Quality reduction requires sponsor approval | Quality reduction unacceptable to sponsor | Project end item is effectively useless |

## 1- Scenario analysis

Documentation of scenario analyses can be seen in various risk assessment forms used by companies. Figure 7.6 is a partial example of a risk assessment form used on an IS project involving the upgrade from Windows Vista to Windows 7.

Notice that in addition to evaluating the severity and probability of risk events the team also assesses when the event might occur and its detection difficulty. Detection difficulty is a measure of how easy it would be to detect that the event was going to occur in time to take mitigating action, that is, how much warning would we have?

So in the Windows 7 conversion example, the detection scale would range from 5 = no warning (The highest detection score of 5 would be given to events that could only be discovered after it is too late (i.e., system freezing)) to 1 = lots of time to react.

Figure 7.6: Risk Assessment Form

| Risk Event              | Likelihood | Impact | Detection Difficulty | When             |
|-------------------------|------------|--------|----------------------|------------------|
| Interface problems      | 4          | 4      | 4                    | Conversion       |
| System freezing         | 2          | 5      | 5                    | Start-up         |
| User backlash           | 4          | 3      | 3                    | Postinstallation |
| Hardware malfunctioning | 1          | 5      | 5                    | Installation     |

### 1- Scenario analysis

Often organizations find it useful to categorize **the severity** of different risks into some form of risk assessment matrix. The matrix is typically structured around the impact and likelihood of the risk event. For example, the risk matrix presented in Figure 7.7 consists of a 5 x 5 array of elements with each element representing a different set of impact and likelihood values.

The matrix is divided into red, yellow, and green zones representing major, moderate, and minor risks, respectively. The red zone is centered on the top right corner of the matrix (high impact/high likelihood), while the green zone is centered on the bottom left corner (low impact/low likelihood).

The moderate risk, yellow zone extends down the middle of the matrix. Since impact is generally considered more important than likelihood (a 10 percent chance of losing \$1,000,000 is usually considered a more severe risk than a 90 percent chance of losing \$1,000), the red zone (major risk) extends farther down the high impact column.

Using the Windows 7 project again as an example, interface problems and system freezing would be placed in the red zone (major risk), while user backlash and hardware malfunctioning would be placed in the yellow zone (moderate risk).

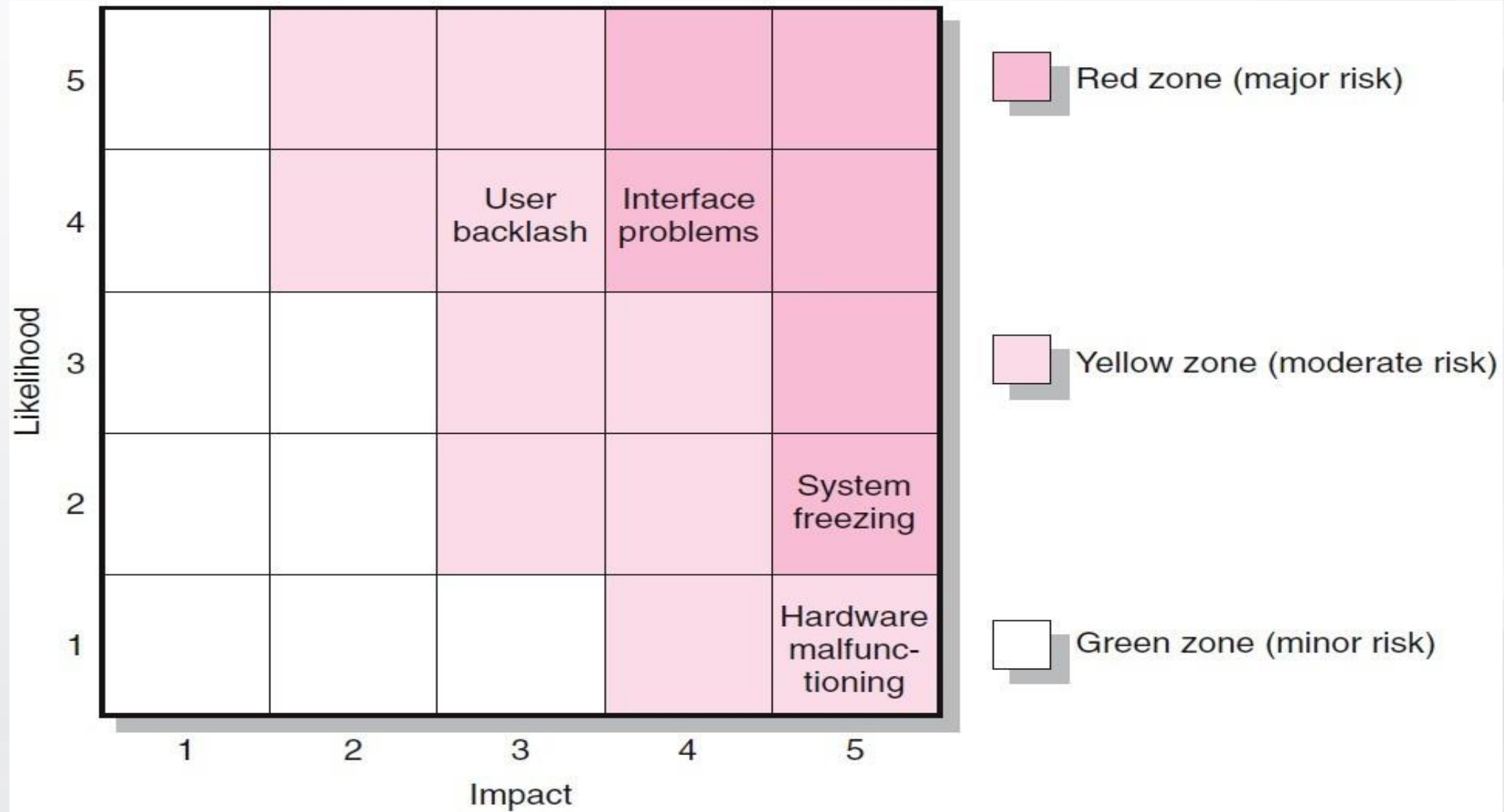
Using the Windows 7 project again as an example, interface problems and system freezing would be placed in the red zone (major risk), while user backlash and hardware malfunctioning would be placed in the yellow zone (moderate risk). The **risk severity matrix** provides a basis for prioritizing which risks to address. Red zone risks receive first priority followed by yellow zone risks. Green zone risks are typically considered inconsequential and ignored unless their status changes.

***Failure Mode and Effects Analysis (FMEA)*** extends the risk severity matrix by including ease of detection in the equation:

$$\text{Impact} \times \text{Probability} \times \text{Detection} = \text{Risk Value}$$

For example, a risk with an impact in the “1” zone with a very low probability and an easy detection score might score a 1 ( $1 \times 1 \times 1 = 1$ ). Conversely, a high-impact risk with a high probability and impossible to detect would score 125 ( $5 \times 5 \times 5 = 125$ ). This broad range of numerical scores allows for easy stratification of risk according to overall significance.

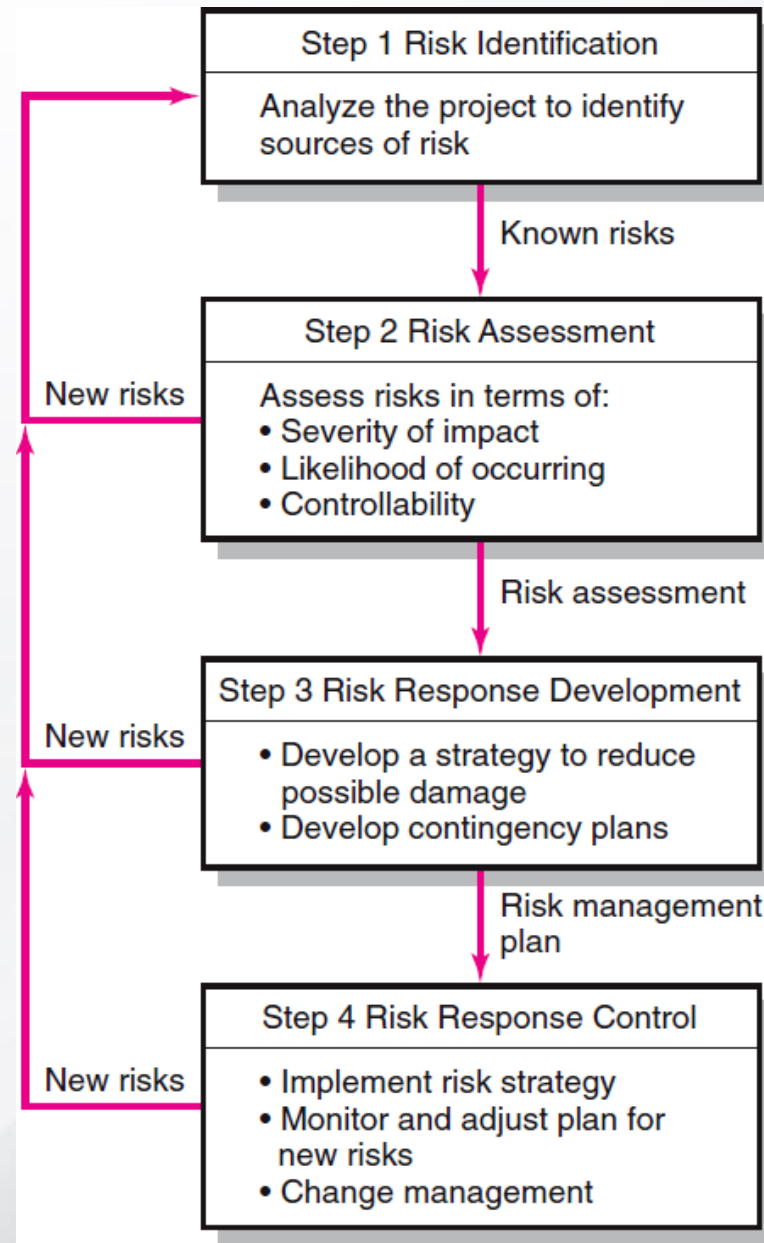
**FIGURE 7.7**  
**Risk Severity Matrix**



No assessment scheme is **absolutely foolproof**. For example, the weakness of the *Failure Mode and Effects Analysis* (FMEA) approach is that a risk event rated Impact=1, Probability =5, and Detection=5 would receive the same weighted score as an event rated Impact= 5, Probability = 5, and Detection = 1! This underscores the importance of *not* treating risk assessment as simply an exercise in mathematics. There is no substitute for thoughtful discussion of key risk events.

## 2- Probability Analysis

There are many statistical techniques available to the project manager that can assist in assessing project risk. Decision trees have been used to assess alternative courses of action using expected values. Statistical variations of net present value (NPV) have been used to assess cash flow risks in projects.



**FIGURE 7.2**  
**The Risk Management Process**

**FIGURE 7.2**

### Step 3: Risk Response Development

When a risk event is identified and assessed, a decision must be made concerning which response is appropriate for the specific event.

Responses to negative risk can be classified as mitigating, avoiding, transferring, or retaining.

#### 1- Mitigating Risk

Reducing risk is usually the first alternative considered. There are basically two strategies for mitigating risk: **(1) reduce the likelihood that the event will occur** and/ or **(2) reduce the impact that the adverse event would have on the project**. Most risk teams focus first on reducing the likelihood of risk events since, if successful, this may eliminate the need to consider the potentially costly second strategy.

**(1) An example of reducing the probability of risks occurring** are testing and prototyping are frequently used to prevent problems from surfacing later in a project. An example of testing can be found in an information systems project. The project team was responsible for installing a new operating system in their parent company. Before implementing the project, the team tested the new system on a smaller isolated network. By doing so they discovered a variety of problems and were able to come up with solutions prior to implementation. The team still encountered problems with the installation, but the number and severity were greatly reduced.

**(2) An alternative mitigation strategy is to reduce the impact of the risk if it occurs.** For example, a bridge-building project illustrates risk reduction. A new bridge project for a coastal port was to use an innovative, continuous cement-pouring process developed by an Australian firm to save large sums of money and time. The major risk was that the continuous pouring process for each major section of the bridge could not be interrupted. Any interruption would require that the whole cement section (hundreds of cubic yards) be torn down and started over.

An assessment of possible risks centered on delivery of the cement from the cement factory. Trucks could be delayed, or the factory could break down. Such risks would result in tremendous rework costs and delays. Risk was reduced by having two additional portable cement plants built nearby on different highways within 20 miles of the bridge project in case the main factory supply was interrupted. These two portable plants carried raw materials for a whole bridge section, and extra trucks were on immediate standby each time continuous pouring was required. Similar risk reduction scenarios are apparent in system and software development projects where parallel innovation processes are used in case one fails.

## 2- Avoiding Risk

- Risk avoidance is changing the project plan to eliminate the risk or condition. Although it is impossible to eliminate all risk events, some specific risks may be avoided before you launch the project. For example, adopting proven technology instead of experimental technology can eliminate technical failure.
- Risk avoidance eradicates the risk by removing the risk or its cause.
- Risk avoidance is most suitable in the early stages of a project, through improved communications, additional resources, or more-clearly defined scope.

### 3- Transferring Risk

Passing risk to another party is common; this transfer does not change risk. Passing risk to another party almost always results in paying a premium for this exemption. **Fixed-price contracts** are the classic example of transferring risk from an owner to a contractor. The contractor understands his or her firm will pay for any risk event that materializes; therefore, a monetary risk factor is added to the contract bid price. Before deciding to transfer risk, the owner should decide which party can best control activities that would lead to the risk occurring contractor capable of absorbing the risk? Clearly identifying and documenting responsibility for absorbing risk is imperative. Another more obvious way to transfer risk is **insurance**.

#### 4- Retaining Risk

In some cases, a conscious decision is made to accept the risk of an event occurring. Some risks are so large it is not feasible to consider transferring or reducing the event (e.g., an earthquake or flood). The project owner assumes the risk because the chance of such an event occurring is slim. In other cases risks identified in the budget reserve can simply be absorbed if they materialize. The risk is retained by developing a contingency plan to implement if the risk materializes. In a few cases a risk event can be ignored and a cost overrun accepted should the risk event occur.

The more effort given to risk response before the project begins, the better the chances are for minimizing project surprises.

# Solved Exercise: Three Types of Software Risk

Threaten the project plan. I.e. if the risks materialize, then it is likely that the project schedule will slip and costs will increase.

- Budgetary/funding

- Schedule

- Personnel issues

- Resources

- Project plan

Hardware

Environmental risk

## **Business Risks**

Threaten the viability of the product to be built.

- Building a great product that no-one wants anymore. (Market risk)
- Building a product that no longer fits into the overall business strategy for the company (Strategic risk).
- Building a product that the sales force doesn't understand how to sell.
- Losing the support of senior management due to a change in focus or a change in people. (Management risk).
- Losing budgetary or personnel commitment (Budget risk)
- Contracts
- Political concerns
- Legal risk

**Technical Risks**

Threaten the quality and timeliness of the software to be produced.

Design

Implementation

Interfacing

Verification

Cutover

Maintenance

**Security**



# Thank You