UNIT - 5 Date .....

Chapter 35
Risk Management

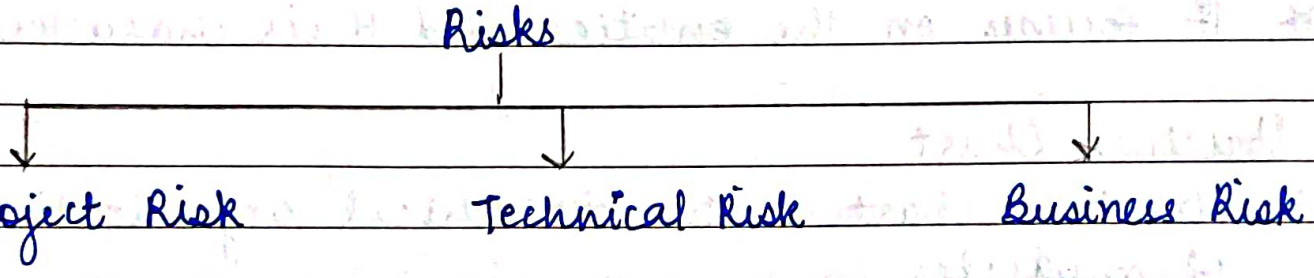
Reactive versus Proactive Risk Strategies

Reactive : Mitigate severity of safety events and threats
Proactive : Identify safety concerns before safety events happen.

Software Risks

Risks involves 2 characteristics :

1. Uncertainity - Risks may or may not happen
2. Loss - If risks becomes reality, undesirable consequences are bound to occur.



1. Project Risks

* Project risks threaten the project plan. If this risk becomes reality then schedule may slip and you'll have over budget.

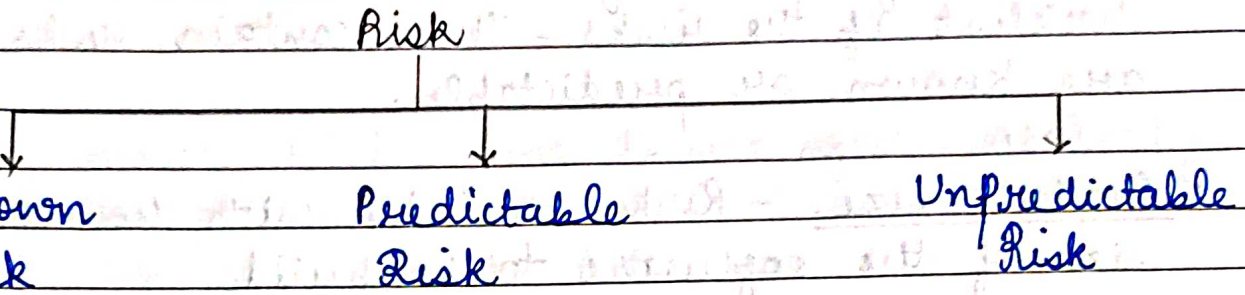
2. Technical Risks

* Technical risks threaten the quality and timeliness of the software to be produced.
* If the risk becomes reality then implementation will be difficult or almost impossible.

Date .....

3. Business Risk

* Business risk threaten the viability of the software to be build.
* If this risk becomes a reality then the product that we have developed has no customers.



1. Known Risk - This can be uncovered after careful evaluation of the plan.

2. Predictable Risk - These are extrapolated from past project experience. Example: Staff turnoves, poor communication with the customers.

3. Unpredictable Risk - These are extremely difficult to identify in advance.

Risk Identification.

Risk identification is a systematic attempt to specify threats to the project plan.

There are 2 distinct types of risks for each of the categories:

1. Generic Risk

They are potential threat to every software project.

Date .....

2. Product Specific risk
These are identified with respect to people, technology and environment that are specific to the project.

* For identification of the risk create a checklist of the risks - These contain risks that are known or predictable.

- Product Size. - Risk associated with the overall size of the software to be build.
- Business Impact - Risks associated with constraints imposed by management or the market place.
- Stakeholder characteristics - Risks associated with the sophistication of the stakeholders and the developer's ability to communicate with stakeholders in a timely manner.
- Process definition - Risks associated with the degree to which the software process was designed and followed.
- Development Environment - Risks associated with the availability and quality of the tools to be used to build the ~~proj~~ product.
- Technology to be build - Risks associated with the complexity of the S/W to be build and the "newness" of the technology that is packaged by the system.

Spiral

Date .....

- Staff size and experience — Risks associated with the overall technical and project experience of the software engineers who will do the work

Risk Components

The risk components are defined in the following manner:

- Performance Risk — The degree of uncertainity that the product will meet its requirements and be fit for its intended use.
- Cost Risk — The degree of uncertainity that the project budget will be maintained.
- Support Risk — The degree of uncertainity that the resultant software will be easy to correct, adapt and enhance.
- Schedule Risk — The degree of uncertainty that the project schedule will be maintained and the product will be delivered on time.

Impact of these risks.

→ Catastrophic — If project cost increases by approx 500K dollars.
→ Critical — If increased project cost is lying b/w $100K to $500K.
→ Marginal — If the project cost increased to $1K to $100K.
→ Negligible — If increased cost is less than $1K.

Spiral

Date .....

Risk Projection

Also called risk estimation, attempts to rate each risk in 2 ways:

1. the likelihood or probability that the risk is real and will occur.
2. Consequences of the problems associated with the risk., should it occur.

4 Risk Projection Steps.

1. Establish a scale that reflects the perceived likelihood of a risk.
2. Delineate the consequences of the risk.
3. Estimate the impact of the risk on the project and the product.
4. Assess the overall accuracy of the risk projection so that there will be no misunderstandings

Risk Table

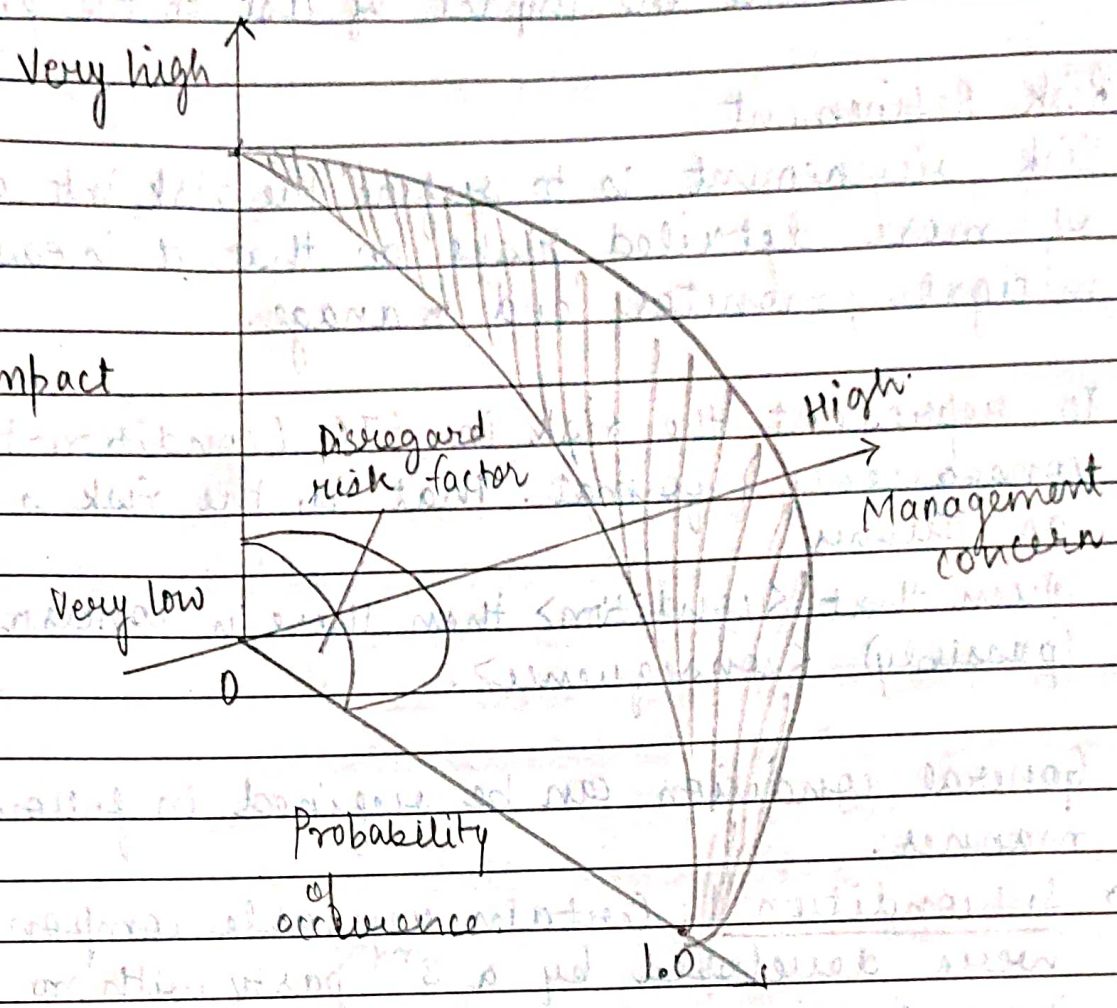
The risk table gives a project manager a method for risk projection.

→ The first column of the table, a project team begins by outlining all risks.
→ The second column of categorizes the threat.
→ The chance / likelihood is placed in the 3rd column of the table.
→ The impact of the risk is then evaluated.
→ The fourth column specifies RMMM.

What risks can happen	Category of risk	Probability of risk	Impact of Risk	RMMM

Date .....

Risk and management Concern.



Assessing Risk Impact.

* Three factors affect the consequences that are likely if a risk does occur:
  1. Nature - Indicates the problems that are likely if it occurs.
  2. Scope - Combines the severity with its overall distribution
  3. Timing - when and for how long the impact will be felt.

* Also called risk exposure. (RE)

$$RE = P \times C.$$

P → Average probability of occurrence value for

Date .....

each risk component.
C → Determine the impact of cost to the project.

Risk Refinement

* Risk refinement is to refine the risk into a set of more detailed risks so that it is easier to mitigate, monitor and manage.

* To represent the risk in CTC (condition-transition consequence) format. That is, the risk is stated as follows:
Given that <condition> then there is concern that (possibly) <consequence>.

* General condition can be refined in following manner:
→ Subcondition 1: Certain reusable components were developed by a 3rd party with no knowledge of internal design standards.
→ Subcondition 2: The design standard for component interfaces has not been solidified and may not confirm to certain existing reusable components.
→ Subcondition 3: Certain reusable components have been implemented in a language that is not supported on the target environment.

Risk Mitigation, Monitoring and Management

* If a software team adopts a proactive approach to risk, avoidance is always the best strategy. This is achieved by developing a plan for risk mitigation.

Date .....

To mitigate the risk for reducing the staff turnover:

1. meet with current staff to determine causes for turnover.
2. mitigate those causes that are under your control before the project starts.
3. Once the project commences, assume turnover will occur and develop techniques to ensure continuity when people leave.
4. Organize project teams so that information about each development activity is widely dispersed.
5. Define work product standards and establish mechanisms to be sure that all models and documents are developed in a timely manner.
6. Conduct peer reviews of all work.
7. Assign a backup staff member for every critical technologist.

* Risk monitoring activities will provide an indication of whether the risk is becoming more or less likely. In the case of high staff turnover, risk monitoring will include looking at the attitude of the members based on project pressure, how much team has jelled together, interpersonal relationships among team members, potential problems with compensation and benefits, and availability of jobs with the company & outside.

* Risk management and contingency planning assume that mitigation efforts have failed and risk has become reality. If the mitigation strategy has been followed, backup is available, information is documented

Spiral

Date .....

The RMMM Plan

- The RMMM Plan documents all work performed as part of risk analysis and is used by the project manager as part of the overall project plan
- When the RMMM has been documented and project has begun, risk mitigation and monitoring steps commence.