Risk Management

Project Risks

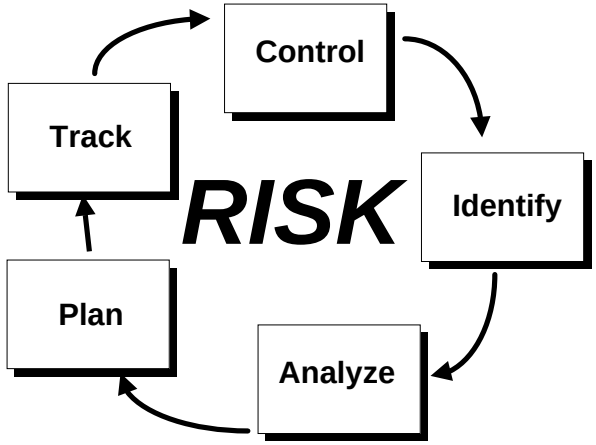
Characteristics of Risks

- Uncertainty
- Loss

Why Software Development has Risks?

- Novel
- Complex
- New technology
- Involve many people
- Specialist expertise
- Methods

Risk Management Paradigm



Stages of Risk Analysis

- Identify
- Characterize
- Quantify
- Assess
- Plan Risk Aversion

Reactive Risk Strategies

- Most software teams rely solely on reactive strategies.
- The team closely monitors the project for likely risks.
- Resources are set aside to deal with them.
- More commonly, the software team does nothing about risks until something goes wrong.
- The team flies into action to correct the problem rapidly.
- This is called fire fighting mode.

Reactive Risk Management

- Project team reacts to risks when they occur
  - **Mitigation** — Plan for additional resources in anticipation of fire fighting
  - **Fix on Failure** — Resource are found and applied when the risk strikes
  - **Crisis Management** — Failure does not respond to applied resources and project is in jeopardy

Proactive Risk Strategies

- More intelligent strategy.
- This begins long before technical work initiated. Potential risks are identified, their probability and impact are assessed and they are ranked by importance.
- The team establishes a plan for managing risk.
- The primary objective is to avoid risk, but because not all risks can be avoided, the team works to develop a contingency plan that will enable it to respond in controlled and effective manner.

Proactive Risk Management

- Formal risk analysis is performed
- Organization corrects the root causes of risk
  - Total Quality Management (TQM) concepts and statistical Software Quality Assurance (SQA)
  - Examining risk sources that lie beyond the bounds of the software
  - Developing the skill to manage change

Proactive Risk Management

- After estimation of effort, duration and cost, it is need to decide go on the project or not.
- Making decision to go on without analyzing risks only means that risks will have to be faced after they have materialized into problems without preparations.

Risk Mitigation, Monitoring, and Management

- **Mitigation** — how can we avoid the risk?
- **Monitoring** — what factors can we track that will enable us to determine if the risk is becoming more or less likely?
- **Management** — what contingency plans do we have if the risk becomes a reality?

Risk Mitigation, Monitoring, and Management

- To avoid the risks an effective strategy must consists of three issues :
  - Risk Avoidance
  - Risk Monitoring
  - Risk Management and Contingency Planning

Risk Mitigation, Monitoring, and Management

- The best strategy is **Risk Avoidance**. This is achieved by developing a plan for risk mitigation.
- As project proceeds, **Risk Monitoring** activities commence. The project manager monitors that may provide an indication of whether the risk is becoming more or less likely.
- **Risk Management and Contingency Planning** assumes that mitigation efforts have failed and that risk has become a reality.

Risk Mitigation, Monitoring and Management Plan

- Risk Mitigation, Monitoring and Management (RMMM) Plan documents all work performed a part of the risk analysis and is used by the project manager as part of the overall project plan.

Risk Table

- The project manager studies the resultant sorted table and defines a cut off line.
- The cut off line (drawn horizontally at some point in the table) implies that only risks that lie above the line will be given further attention.
- The risks below the line are re-evaluated to accomplish second-order prioritisation.
- All risks that lie above the cut off line must be managed.

Risk Table

- The last column RMMM is a pointer to Risk Mitigation, Monitoring and Management Plan.
- RMMM is the collection of risk information sheets developed for all risks that lie above the cut off.
- Risk probability can be determined by making individual estimates and then developing a single consensus value. More sophisticated techniques are also available now a days.
- Probability of 0.7 to 1.0 implies a high probable risk.

Component Factors for Impact Ratings

- The nature of the consequences (e.g. staff turnover hit design throughput, cause slippage & additional cost, and affect quality)
- The severity (i.e. how serious would be an occurrence?)
- The distribution (i.e. how wide would be the implications?)
- The timing (i.e. when would it occur?)
- The duration (i.e. how long would it be felt?)

Building the Risk Table

- Estimate the probability of occurrence
- Estimate the impact on the project on a scale of 1 to 5
  - 1 = Low impact on project success
  - 5 = Catastrophic impact on project success
- Sort the table by probability and impact

Risk	Probability	Impact	RMMM
			Risk Mitigation Monitoring & Management

Risk Monitoring

- Risk Monitoring involves regularly assessing each of the identified risks to decide whether or not that risk is becoming more or less probable and whether the efforts of the risk have changed.
- Risk monitoring should be a continuous process and, at the management progress review, each of the key risks should be considered separately and discussed by the meeting.

Risk Identification

- Risk identification is a systematic attempt to specify threats to the project plan.
- By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary.
- Risk identification starts with categorization:
  - Business Risks
  - Project Risks
  - Technical Risks
  - Known Risks

Risk Identification – Business Risks

- Example
  - Product clashes with company's strategic aims.
  - Product has no market.
  - Product can't be grasped by salespeople.
  - Loss of upper management support (e.g. change of strategy, change of boss).
  - Loss of resources (e.g. money withdrawn, people withdrawn, equipment withdrawn).

Risk Identification – Project Risks

- Project risks threaten project plan.
- If project risks become real, it is likely that project schedule will slip and costs will increase.
- Project risks identify potential budgetary, schedule, personnel, resource, customer, and requirement problems and their impact on a software project.
- Example:
  - Inadequate customer commitment
  - Incorrect or incomplete requirements
  - Inadequate resource base
  - Too tight a budget
  - Too tight a schedule
  - High staff turnover
  - Inadequate team organization

Risk Identification – Technical Risks

- Technical risks threaten the quality and timeliness of the software to be produced.
- If a technical risk becomes a reality, implementation may become difficult or impossible.
- Technical risks identify potential design, implementation, interfacing, verification, and maintenance problems.
- Technical risks occur because the problem is harder to solve than we through it would be.

Risk Identification – Known risks

- Known risks are those that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed and other reliable information sources
  - E.g. unrealistic delivery date, lack of documented requirements or software scope, poor development environment

Risks Factors

- Hardware
- Software
- Users
- Developers
- Environment
- Time
- Money

Risks due to Product Size

- Attributes that affect risk:
  - Estimated size of the product in LOC or FP?
  - Estimated size of product in number of programs, files, transactions?
  - Percentage deviation in size of product from average for previous products?
  - Size of database created or used by the product?
  - Number of projected changes to the requirements for the product? before delivery? after delivery?
  - Amount of reused software?

Risks due to Business Impact

- Attributes that affect risk:
  - Affect of this product on company revenue?
  - Visibility of this product by senior management?
  - Reasonableness of delivery deadline?
  - Number of customers who will use this product
  - Interoperability constraints
  - Sophistication of end users?
  - Amount and quality of product documentation that must be produced and delivered to the customer?
  - Governmental constraints
  - Costs associated with late delivery?
  - Costs associated with a defective product?

Risks due to Customer

- Questions that must be answered:
  - Have you worked with the customer in the past?
  - Does the customer have a solid idea of requirements?
  - Has the customer agreed to spend time with you?
  - Is the customer willing to participate in reviews?
  - Is the customer technically sophisticated?
  - Is the customer willing to let your people do their job — that is, will the customer resist looking over your shoulder during technically detailed work?
  - Does the customer understand the software engineering process?

Risks due to Process Maturity

- Questions that must be answered:
  - Have you established a common process framework?
  - Is it followed by project teams?
  - Do you have management support for software engineering
  - Do you have a proactive approach to SQA?
  - Do you conduct formal technical reviews?
  - Are CASE tools used for analysis, design and testing
  - Are the tools integrated with one another?
  - Have document formats been established?

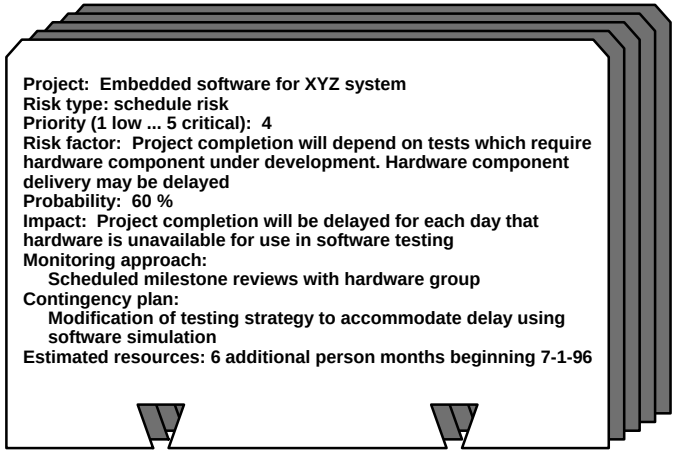
Technology Risks

- Questions that must be answered:
  - Is the technology new to your organization?
  - Are new algorithms, I/O technology required?
  - Is new or unproven hardware involved?
  - Does the application interface with new software?
  - Is a specialized user interface required?
  - Is the application radically different?
  - Are you using new software engineering methods?
  - Are you using unconventional software development methods, such as formal methods, AI-based approaches, artificial neural networks?
  - Are there significant performance constraints?
  - Is there doubt the functionality requested is "do-able?"

Staff/People Risks

- Questions that must be answered:
  - Are the best people available?
  - Does staff have the right skills?
  - Are enough people available?
  - Are staff committed for entire duration?
  - Will some people work part time?
  - Do staff have the right expectations?
  - Have staff received necessary training?
  - Will turnover among staff be low?

Recording Risk Information



Predictable Risks & Unpredictable Risks

- Predictable risks are extrapolated from past project experience
  - E.g. staff turnover, poor communication with the customer, dilution of staff effort as ongoing maintenance requests are serviced
- Unpredictable risks can and do occur, but they are extremely difficult to identify in advance.

Generic Risks & Product-specific Risks

- Generic Risks are a potential threat to every software project.
- Product-specific risks can be identified only by those with a clear understanding of the technology, the people and the environment that is specific to the project at hand.

Risk Projection (Risk Estimation)

- It attempts to rate each risk in two ways - the likelihood or probability that the risk is real and the consequences of the problems associated with the risk.
- The four risk projection activities are
  - Establish a scale that reflects the likelihood of a risk
  - Delineate (portray by drawing) the consequences of the risk
  - Estimate the impact of the risk on the project and the product
  - Note the overall accuracy of the risk projection so that there will be no misunderstandings.

Risk Exposure

- Risk Exposure = P x C
  - P – the probability of occurrence for a risk
  - C – the cost of the project if the risk occur

Risk Assessment

- Defining a likelihood scale (e.g. highly unlikely ... highly likely; 0..1).
- Defining an impact scale.
- Using scale to rate the likelihood & impact for each risk.
- Output
  - A set of Risk Triple (risk, likelihood rating, impact rating)

Risk Assessment

- The next step in risk analysis involves assessing whether the risk levels are acceptable.
- The idea is to correlate the risk triple with break factors & break levels (Risk Referent level) so as to reach a go/no-go decision.