RISK MANAGEMENT

DEF:
"An uncertain event or condition that, if it occurs has a positive or negative effect on a project objectives", include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

- those caused **by the inherent difficulties of estimation;**
- **those due to assumptions made. during the planning process;**
  those of unforeseen (or at least unplanned) events occurring.

DEF:

**1.An uncertain event or condition that if it occurs has a positive or negative effect on a project objectives**

2. The chance of exposure to the adverse consequences of future events'
- Project plans have to be based on assumptions
- Risk is the possibility that an assumption is wrong
- When the risk happens it becomes a problem or an issue

Key elements of risks
- It relates to the future
- It involves cause and effect

CATEGORIES OF RISKS:
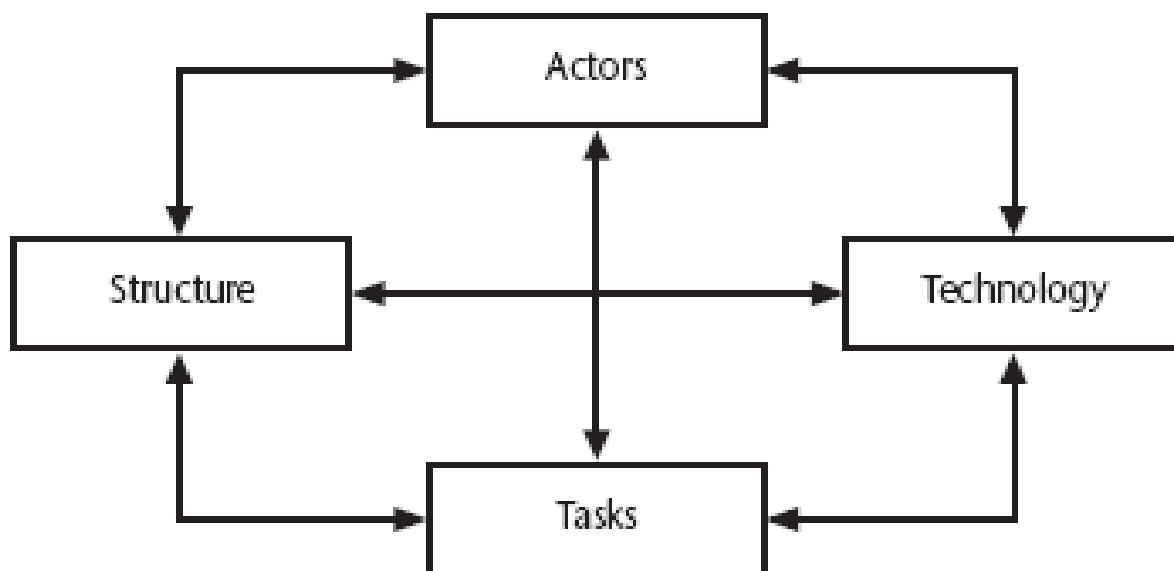
Tasks: the types of task to be undertaken
Structure: the communication systems, management structures, work flows etc
Actor: the people involved in the project
Technology: the methods, techniques and tools to be used

Various types of risks

- **Financial risk** is the loss of key resources like funding, etc. In this case the company will not have adequate cash flow to meet financial obligations. Credit risk, liquidity risk, market risk, operational risk are different types of financial risks.

- When the borrower becomes default and was unable to make payments as promised it is said to be **Credit risk**, also called default risk.

- **Investment risk** was associated with this where the investor losses his principal and interest too. Sometimes due to lack of liquidity in the market an asset cannot be sold to make the profit or to prevent a loss this is what called as **Liquidity risk**.

- Due to the change in value of the market risk factors value of investment portfolio or the value of a trading portfolio will decrease. Foreign exchange rates, stock prices, interest rates, and commodity prices are the standard **Market risk** factors.

- A risk arising from execution of an organisation's business functions is **Operational risk**.

- Risks arising from the people, systems and processes through which an organisation operates. Fraud risks, legal risks, physical or environmental risks are other categories included under this.
- Risky business processes that could lead to project failure are **Process risks**.

- Those risks that are often associated with damage to the reputation of an organisation or its brand are **Intangible risks**.

- Risks which often involve things connected to time are **Time risks**.

- Loss of critical employees or knowledge which are connected to man power are **Human risks**.

- Losses include government regulations and the same having an impact on the operations of the company are **Legal Risks**.

- **Physical risks** are those lose of physical resources such as equipment, buildings, land, etc due to natural disasters or manmade.

Risk management process begins when somebody asks what kind of events can damage the business and how much damage can be done. Identifying and measuring the potential loss exposures, choosing the most efficient methods of controlling and financing loss exposure and implementing them and finally Monitoring all the out comes are the main steps involved in Risk Management.

A FRAMEWORK FOR DEALING WITH RISK
The planning for risk includes these steps:
- Risk identification – what risks might there be?
- Risk analysis and prioritization – which are the most serious risks?

- Risk planning – what are we going to do about them?
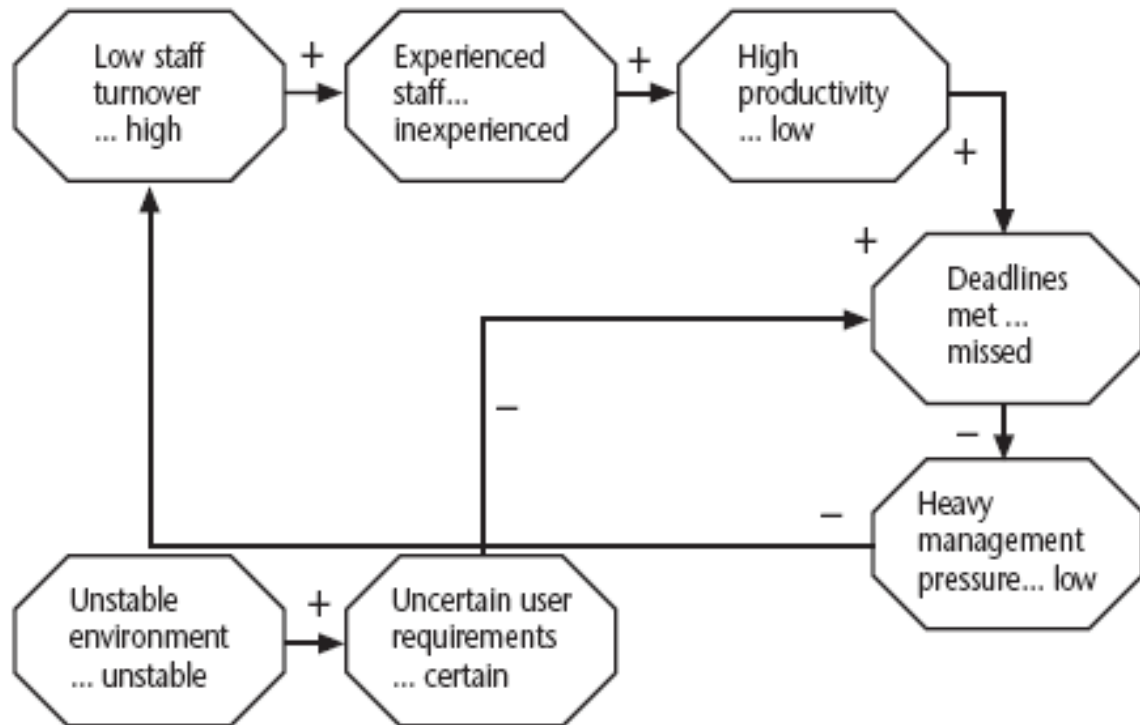- Risk monitoring – what is the current state of the risk?

Risk identification

Approaches to identifying risks include:
- Use of checklists – usually based on the experience of past projects
- Brainstorming – getting knowledgeable stakeholders together to pool concerns
- Causal mapping – identifying possible chains of cause and effect

Boehm's top 10 development risks

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, design to cost
Late changes to requirements	Change control, incremental development
Shortfalls in externally supplied components	Benchmarking, inspections, formal specifications, contractual agreements, quality controls
Shortfalls in externally performed tasks	Quality assurance procedures, competitive design etc
Real time performance problems	Simulation, prototyping, tuning
Development technically too difficult	Technical analysis, cost-benefit analysis, prototyping , training

Causal mapping

Low staff turnover ... high   +   Experienced staff... inexperienced   +   High productivity ... low

+

Deadlines met ... missed

+

−

−

Heavy management pressure... low

−

Unstable environment ... unstable   +   Uncertain user requirements ... certain

Hazard identification
- **A hazard is an event that might occur and will, if it does occur, create a problem for the successful completion of the project**
- **Hazard identification - identify the reasons for failure the activities   List the factors involving the hazard**

Application factors

the nature of the application- whether it is simple data processing applications, a safety –critical system or a large distributed system with real-time elements- is likely to be a critical factor. The expected size of the application is also important.

- **Staff factors: - The experience and skills of the staff involved are clearly major factors- an experienced programmer is, one would hope, less likely to make errors than one with little.**

- **Project factors:- it is important that the project and its objectives are well defined and that they are absolutely clear to all members of the project team and all key stakeholders. Any possibility that is not the case will pose a risk to the success of the project.**
- **Project methods:- using well-specified structured methods(such as PRINCE2) for project management and system development will decrease the risk of delivering a system that is unsatisfactory or late.**
- **Hardware/software factors:- a project that requires new hardware for development is likely to pose a higher risk than one where the software can be developed on existing hardware.**

- **Changeover factors: - the extending to which a project relies on external organizations that cannot be directly controlled often influences the project's success.**
- **Environmental factors: - changes in the environment can affect a project's success.**
- **Health and safety factors:- while not generally a major issue for software projects , the possible effects of project activities on the health and safety of the participants and the environment should be considered.**

Risk Analysis

Risk exposure (RE)= (potential damage) x (probability of occurrence)

Ideally **Potential damage**: a money value e.g. a flood would cause £0.5 millions of damage

Probability 0.00 (absolutely no chance) to 1.00 (absolutely certain) e.g. 0.01 (one in hundred chance)

RE = £0.5m x 0.01 = £5,000

Crudely analogous to the amount needed for an insurance premium

Table 7.1   *Part of Amanda's risk exposure assessment*

	Hazard	Likelihood	Impact	Risk exposure
R1	Changes to requirements specification during coding	1	8	8
R2	Specification takes longer than expected	3	7	21
R3	Staff sickness affecting critical path activities	5	7	35
R4	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	1	10	10

Risk probability: qualitative descriptors

Probability level	Range
High	Greater than 50% chance of happening
Significant	30-50% chance of happening
Moderate	10-29% chance of happening
Low	Less than 10% chance of happening

Qualitative descriptors of impact on cost and associated range values

Impact level	Range
High	Greater than 30% above budgeted expenditure
Significant	20 to 29% above budgeted expenditure
Moderate	10 to 19% above budgeted expenditure
Low	Within 10% of budgeted expenditure.

Probability impact matrix
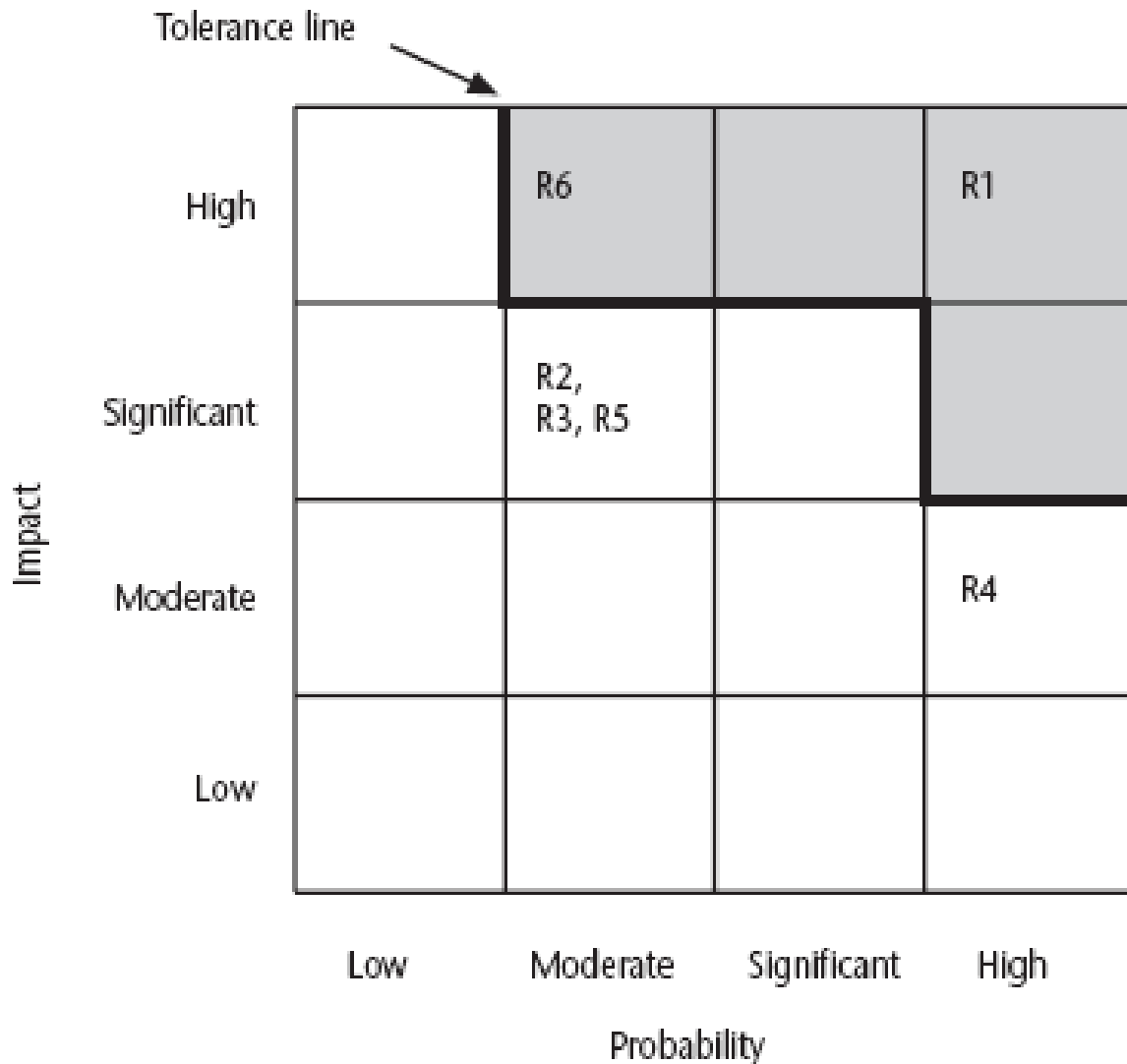
Risk planning.
Risk planning consists of drawing up contingency plans and where appropriate, adding these to the project's task structure. With small projects, risk planning is likely to be the responsibility of the project manager, but medium or large projects will benefit from the appointments of a full-time risk manager.

Risk Acceptance: This is deciding to do nothing about the risk. This means you will accept its consequences. 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 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 Reduction and Mitigation:

Risk Reduction: attempts to reduce the likelihood of the risk occurring. For example, **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 Mitigation: is the action taken to ensure that the impact 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 impact of data corruption not its likelihood of happening, in this sense it is a data mitigation measure.

Risk Transfer: In this case the risk is transferred to another person or organization. For Example, a software development task is outsourced for a fixed fee. Another example is when you buy insurance

Risk reduction leverage

Risk reduction leverage =

$$(RE_{before} - RE_{after}) / (\text{cost of risk reduction})$$

RE_{before} is risk exposure before risk reduction e.g. 1% chance of a fire causing £200k damage
RE_{after} is risk exposure after risk reduction e.g. fire alarm costing £500 reduces probability of fire damage to 0.5%
RRL = (1% of £200k)-(0.5% of £200k)/£500 = 2
RRL > 1.00 therefore worth doing