Risk Management and category of risks

Every project involves risk. Risk is "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.

Some definitions of risk

- 'the chance of exposure to the adverse consequences of future events' PRINCE2
- 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*

Risk Occurs:

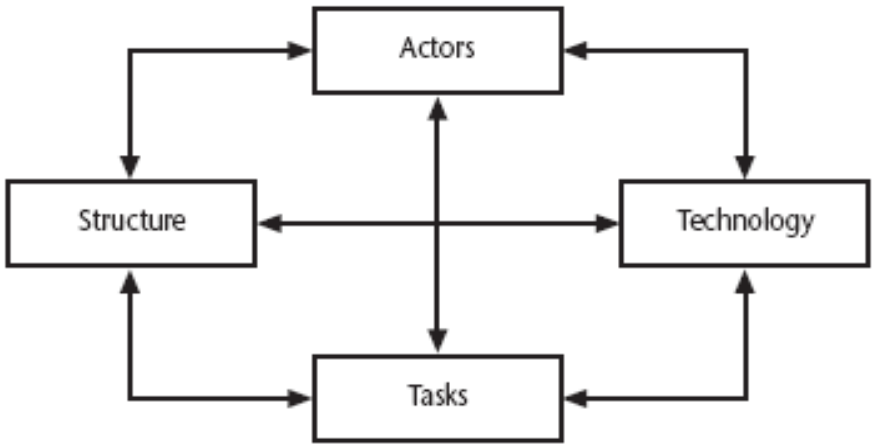
- When the project exceed its original specification
- Deviations from achieving it objectives and so on.

There are two types of risks.

1. **Project risk** – which prevent the project from being completed successfully. Project risk are those could prevent achievement of objectives given to the project manager & project team.
2. **Business risk** – delivered products are not profitable. Economic downturn or import of cheaper alternative products.

- Risk evaluation is meant to decide whether to proceed with the project or not, and whether the project is meeting its objectives.
- Uncertain event or condition that if it occurs has positive or negative condition on project objectives.
- Key elements of Risk follows:-
  - **It relates to the future**-risk involves speculating about future events.
  - **Involves cause & effects**

Categories of risk:



This is based on Lyytinen's socio technical model of risk

- **Actors** relate to all those involved in the project including both developers, users and managers
    - Includes various department specialists, user groups, managers with different responsibilities.
    - If developer builds software components & leave before testing, team member taking over that component find lack of familiarity with software make correction of faults difficult.
    - e.g. a risk could be that high staff turnover leads to information of importance to the project being lost
- **Technology** – both that used to implement the project and that embedded in the project deliverables – risk could be that the technologies selected are not in fact appropriate.
- **Structure** – this includes management procedures, risk here is that a group who need to carry out a particular project task are not informed of this need because they are not part of the project communication network
- **Tasks** – the work to be carried out. A typical risk is that the amount of effort needed to carry out the task is underestimated.

A risk could be well belong to more than one of the four areas – for example, estimates being wrong could be influenced by problems with actors (e.g. lack of experience with a technical domain) or the structure (over optimism of managers keen to win work).

Some other categories of risks:

- **Schedule Risk**
  - Wrong time estimation
  - Resources are not tracked properly. All resources like staff, systems,skills of individuals etc.
  - Unexpected project scope expansions
- **Budget Risk**
  - Wrong budget estimation
  - Cost overruns
  - Project scope expansion
- **Operational Risks**
  - No proper subject training
  - No resource planning
  - No communication in team.
- **Technical risks**
  - Product is complex to implement.
  - Difficult project modules integration.
  - Continuous changing requirements
- **Programmatic Risks**
  - Market development
  - Changing customer product strategy and priority
  - Government rule changes

ISPL situational factors: the target domain

1. **Information system -** the characteristics of the information system - these areindependent of the technologies that might be used
2. **Computer system -** the characteristics of the part of the information systemthat have been computerized

ISPL situational factors: project domain

Project	• the types of task to be undertaken
Structure	• the communication systems, management structures, work flows etc
Actors	• the people involved in the project
Technology	• the methods, techniques and tools to be used

Managing Risk

The proactive management of risks throughout the software development lifecycle is important for project success. In this chapter, we will explain the following:

- the risk management practice, which involves risk identification, analysis, prioritization, planning, mitigate on, monitoring, and communication
- software development risks that seem to reoccur in educational and industrialprojects
- a risk-driven process for selecting a software development model

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

Checklists

- ✓ They are simply lists of the risks have been found to occur regularly in softwaredevelopment projects
- ✓ Creators of checklists also suggest potential counter measures for each risk.
- ✓ If manager identifies risk ,he can use counter measures to cope with them.

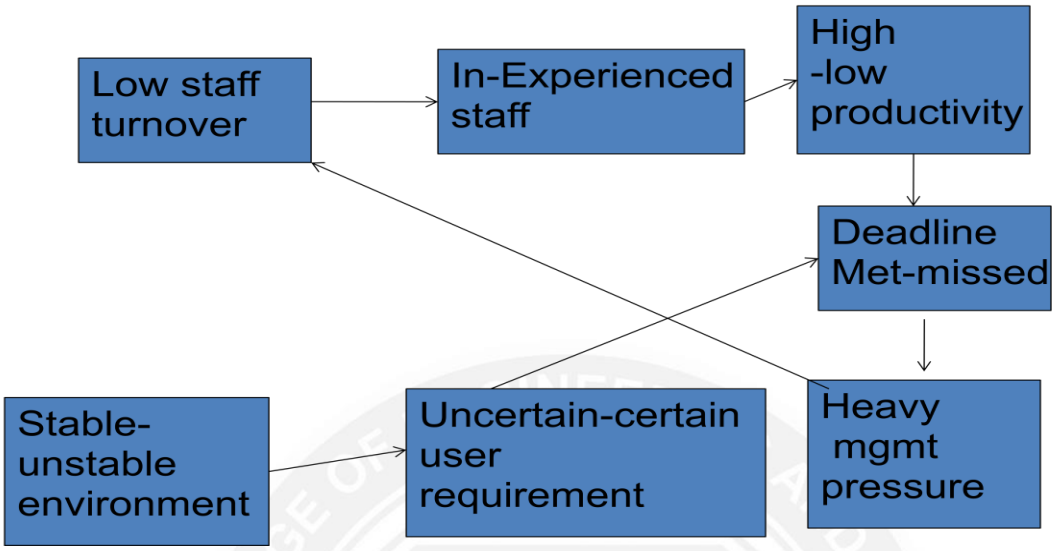
Brain storming

- ✓ Representative of main stakeholders can be brought together ,and a plan isdrafted.
- ✓ It is used to identify the possible solutions to the problem.
- ✓ All stakeholders have a meeting and risk in the projects are discussed.

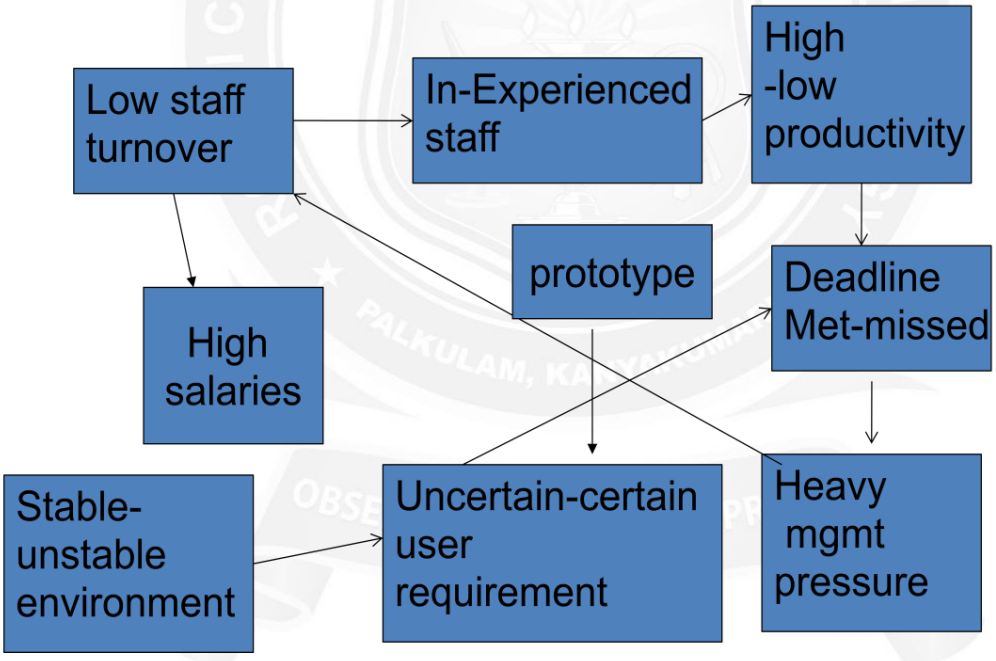
Casual mapping

- ✓ One way of identifying possible threats to the success of a project & measuresthat might eliminate & reduce them is the use of casual mapping.
- ✓ Casual maps & diagrams represent chains of causes & effects that will influence outcomes in particular area

✓ Example: Casual map of problem area



Casual map of problem area with solution



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 inhundred chance)

If there were 100 people chipping in £5,000 each, there would be enough for the 1 in100 chance of the flooding. If there were 2 floods then the system collapses! Exercise

in the textbook is strongly recommended to explore these issues. In practice, with project risks, these quantitative approaches are usually impractical and more qualitative approaches are used instead. See the next overhead.

RE = £0.5m x 0.01 = £5,000

Crudely analogous to the amount needed for an insurance premium

	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

Table: Part of Amanda risk exposure assessment

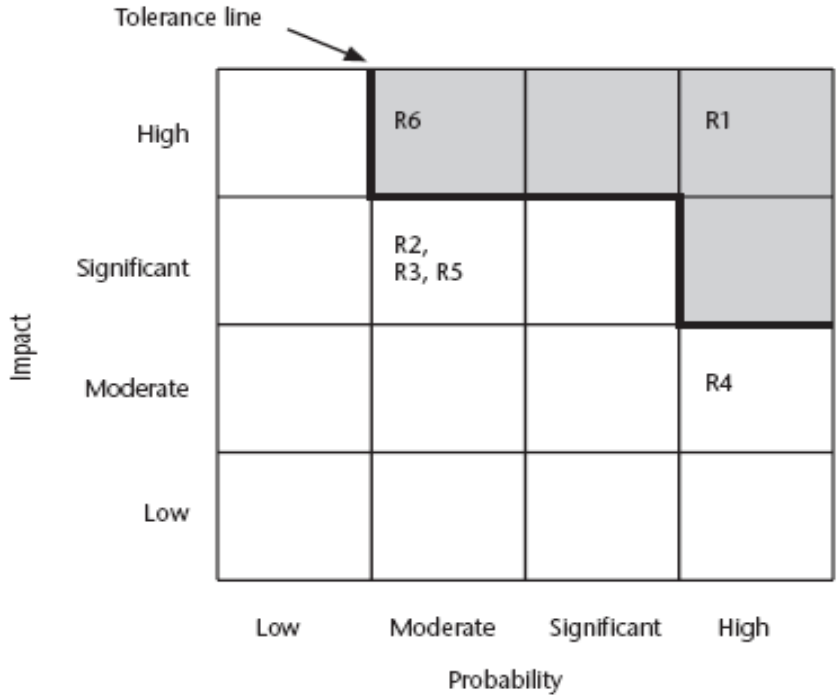
Table: Risk probability: qualitative descriptors

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**

Table: 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



- R1, R2 etc refer to particular risks (See Table 7.4 in the textbook). They are located on the grid according to the likelihood and impact ratings that have been allocated to them. A zone around the top right hand corner of the grid can be designated and risks falling within that zone are treated as requiring urgent action.

Risk planning:

Risks can be dealt with by:

- **Risk acceptance –** the cost of avoiding the risk may be greater than the actual cost of the damage that might be inflicted
- **Risk avoidance –** avoid the environment in which the risk occurs e.g. buying an OTS application would avoid a lot of the risks associated with software development e.g. poor estimates of effort.
- **Risk reduction –** the risk is accepted but actions are taken to reduce its likelihood e.g. prototypes ought to reduce the risk of incorrect requirements
- **Risk transfer –** the risk is transferred to another person or organization. The risk of incorrect development estimates can be transferred by negotiating a fixed price contract with an outside software supplier.
- **Risk mitigation –** tries to reduce the impact if the risk does occur e.g. taking backups to allow rapid recovery in the case of data corruption

Risk acceptance

- This is do nothing option.
- We would decide that damage inflicted by some risk would be less than cost ofaction.

Risk avoidance

- Some activities are so prone to accidents that it is best to avoid them
- If u are worried about crocodiles then don't go into the water
- When Manager will decide to avoid the risk he will buy an off the shelf components.

Risk reduction

Risk reduction leverage = $(RE_{before} - RE_{after})$/ (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 reducesprobability of fire damage to 0.5%

- If you think in terms of the analogy to insurance. An insurance company mightreduce the fire insurance premium from £2k to £1k on condition that a fire alarm is

installed. The insured would save £1k a year by investing £500 so it would beworth doing.
RRL = (1% of £200k)-(0.5% of £200k)/£500 = 2

RRL > 1.00 therefore worth doing

Risk mitigation

- Risk mitigation is action taken to ensure that impact of risk is lessened when itoccurs.
- It tries to reduce the impact if the risk does occur e.g. taking backups to allow rapid recovery in the case of data corruption

Risk transfer

- Risk is transferred to another person or organization
- With software projects example would be where a software development task isoutsourced to an outside agency for a fixed fee.

Evaluating risk to schedule

- We use PERT technique
- Use to evaluate the effects of uncertainty
- PERT require three estimates
  - ✓ Most likely time
  - ✓ Optimistic time
  - ✓ Pessimistic time
- Most likely time --The time we would expect the task to take under normal circumstances ,denoted by:-m
- Optimistic time—shortest time in which we could expect to complete the activity, denoted by a.
- Pessimistic time—worst possible ,denoted by b

  $t_e=(a+4m+b)/6$
- Calculate standard deviation for each project events $s=(b-a)/6$
- Calculate z value for each event that has target date $z=(T - t_e) /s$

  where

  t_e expected date

  T target date