Software Project Management

Durga Prasad Mohapatra

Professor

CSE Deptt.

NIT Rourkela

Risk management cont…

A Framework for Dealing with Risk

Planning for risk includes these steps:

(i) Risk identification

(ii) Risk analysis and prioritization

(iii) Risk planning

(iv) Risk monitoring

A Framework for Dealing with Risk

- Steps (i) to (iii) will probably be repeated.
- When risks that could prevent a project success are identified, plans can be made to reduce or remove their threat.
- The plans are then reassessed to ensure that the original risks are reduced sufficiently and no new risks inadvertently introduced.

Example

- Consider the risk that staff inexperience with a new technology could lead to delays in software development.
- To reduce this risk, consultants who are expert in the new technology might be recruited.
- However, the use of consultants might introduce the new risk that knowledge about the new technology is not transferred to the permanent staff, making subsequent software maintenance problematic.
- Having identified this new risk, further risk reduction activities can be planned.

Risk Identification

There are two main approaches to the identification of risks:

- ✓ use of checklists
- ✓ brainstorming

Checklists

- Checklists are simply lists of the risks that have been found to occur regularly in software development projects.
- A specialized list of software development risks by Barry Boehm appears in the next table in a modified version.
- Ideally a group of representative project stakeholders examines a checklist identifying risks applicable to their project.
- Often the checklist suggests potential countermeasures for each risk.

Software project risks and strategies of Risk reduction

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

Software project risks and strategies of Risk reduction cont..

Risk	*Risk reduction techniques*
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

Checklists

- Project management methodologies, such as PRINCE2, often recommend that on completion of a project a review identifies any problems during the project and the steps that were (or should have been) taken to resolve or avoid them.
- In some cases, these problems could be added to an organizational risk checklist for use with new projects.

Brainstorming

- Ideally, representatives of the main stakeholders should be brought together once some kind of preliminary plan has been drafted.
- Then, they identify, the problems that might occur, using their individual knowledge of different parts of the project.

Risk Assessment

- A common problem with risk identification is that a list of risks is potentially endless.
- A way is distinguishing the damaging and likely risks. This can be done by estimating the risk exposure for each risk using the following formula:

risk exposure = (potential damage) X (probability of occurrence)

Risk Assessment

- Usually, the potential damage is assessed as a money value.
- Example: Suppose, a project depends on a data centre vulnerable to fire. It might be estimated that if a fire occurred a new computer configuration could be established for £500,000. It might also be estimated that where the computer is located there is a 1 in 1000 chance of a fire actually happening, that is a probability of 0.001.
- Then, the risk exposure in this case would be:

£500,000 X 0.001 = £500

Risk Assessment

- A crude way of understanding this value is as the minimum sum an insurance company would require as a premium.
- If 1000 companies, all in the same position, each contributed £500 to a fund then, when the 1 in 1000 chance of the fire actually occurred, there would be enough money to cover the cost of recovery.

Risk Assessment

- The calculation of risk exposure assumes that the amount of damage sustained will always be the same. However, it is usually the case that there could be varying amounts of damage.
- For example, as software development proceeds, more software is created, and more time would be needed to re-create it if it were lost.
- With some risks, there could be not only damage but also gains. The testing of a software component is scheduled to take six days, but is actually done in three days. A team leader might therefore feel justified in producing a probability chart for this.

Risk Assessment

- Most managers resist very precise estimates of loss or of the probability of something occurring, as such figures are usually guesses. Barry Boehm has suggested that, because of this, both the risk losses and the probabilities be assessed using relative scales in the range 0 to 10.
- The two figures could then be multiplied together to get a notional risk exposure.
- Next table provides an example, of where this has been done. This value could be used to prioritize the importance of risks, although more sophisticated risk calculations are not possible.

Example for risk exposure assessment

Ref	Hazard	Likelihood	Impact	Risk
R1	Changes to requirements specification during coding	8	8	64
R2	Specification takes longer than expected	3	7	21
R3	Significant staff sickness affecting critical path activities	5	7	35
R4	Significant 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	4	8	32

Another approach for risk exposure assessment

- Even using indicative numbers in the range 0 to 10, rather than precise money values and probabilities, is not completely satisfactory. The values are likely to be subjective, and different analysts might pick different numbers.
- Another approach is to use qualitative descriptions of the possible impact and the likelihood of each risk (see next tables, for examples). Consistency between assessors is facilitated by associating each qualitative description with a range of values.

Qualitative descriptors of risk probability and associated range values

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

Probability 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

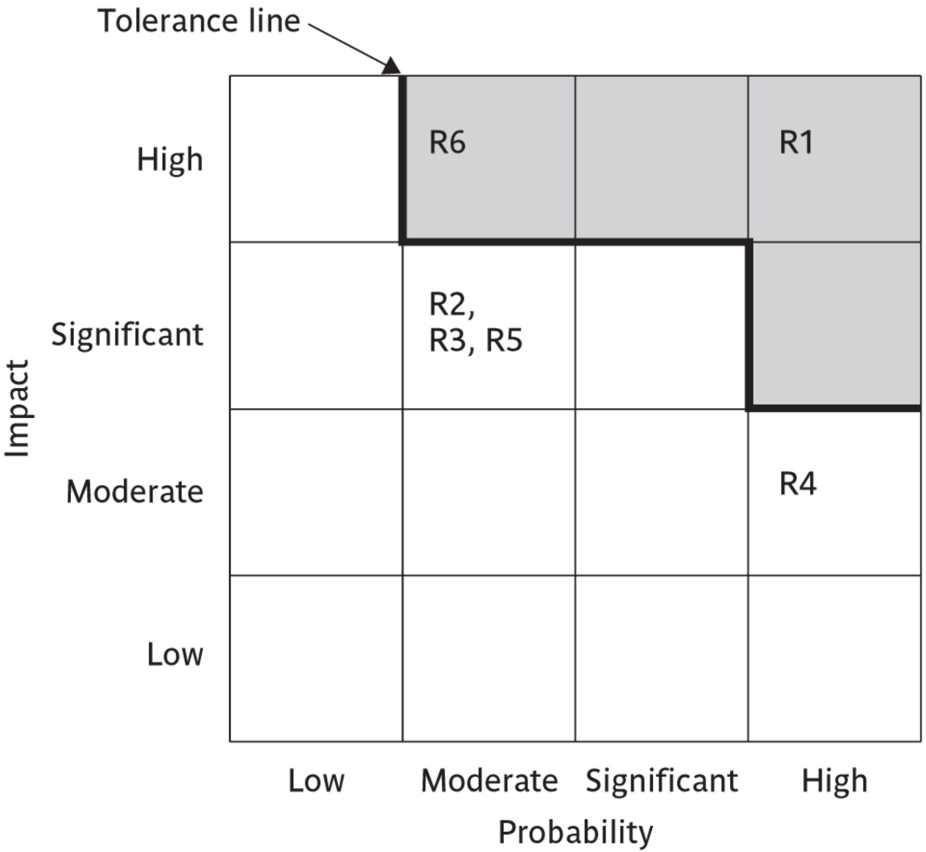
Another approach for risk exposure assessment

- In the later table, the potential amount of damage has been categorized in terms of its impact on project costs. Other tables could be drawn to show the impact of risks on project duration or on the quality of the project deliverables.
- To some extent, the project manager, in conjunction with the project sponsor, can choose whether the damage inflicted by a risk affects cost, duration or the quality of deliverables.

Probability impact matrix

- Where the potential damage and likelihood of a risk are defined by qualitative descriptors, the risk exposure cannot be calculated by multiplying the two factors together. In this case, the risk exposure is indicated by the position of the risk in a matrix (see next figure).
- These matrices have variously been called probability impact grids (matrix) or summary risk profiles.
- In this figure, some of the cells in the top right of the matrix have been zoned off by a tolerance line. Risks that appear within this zone have a degree of seriousness that calls for particular attention.

Probability impact matrix



Impact	Low	Moderate	Significant	High
High		R6		R1
Significant		R2, R3, R5		
Moderate				R4
Low				
	Probability			

Another approach for risk exposure assessment

- We know that there is a need for frequent reassessment of effort and duration estimates during a project. This also applies to risk exposure as well, as some risks apply only at certain stages.
- A risk might be that key users are unavailable when needed to supply details of their requirements. As requirements are gathered, so this risk will diminish until it is no longer significant.
- In general, the element of uncertainty will lessen as a project progresses and more is learnt by the developers about user requirements and any new technology. This would be reflected in lower risk probabilities.

Another approach for risk exposure assessment

- On the other hand, the potential damage will tend to increase as the amount invested in the project grows. If you type a substantial report using a word processor and neglect to take back-ups, as each day adds more text to the report, it also adds to the number of days needed to re-key the report in the event of file loss.

Risk Planning

- Having identified the major risks and allocated priorities, the next task is to decide how to deal with them.
- The choices are:
  - risk acceptance;
  - risk avoidance;
  - risk reduction and mitigation;
  - risk transfer.

Risk acceptance

- This is the do-nothing option. We will already, in the risk prioritization process, have decided to ignore some risks in order to concentrate on the more likely or damaging.
- We could decide that the damage inflicted by some risks would be less than the costs of action that might reduce the probability of a risk happening.

Risk avoidance

- Some activities may be so prone to accident that it is best to avoid them altogether. If you are worried about **sharks** then **don't go into the water**.
- For example, given all the problems with developing software solutions from scratch, managers might decide to retain existing clerical methods, or to buy an off-the-shelf solution.

Risk reduction

- Here we decide to go ahead with a course of action despite the risks, but take precautions that reduce the probability of the risk.
- Suppose, two of the staff scheduled to work on a project departed for other jobs. If this has been identified as a risk, steps might have been taken to reduce possible departures of staff.
- For instance, the developers might have been promised generous bonuses to be paid on successful completion of the project.

Risk reduction

- Suppose, after the purchase of the payroll package, there is a requirement for the payroll database to be accessed by another application. Unfortunately, the application that had been bought did not allow such access.
- An alternative scenario is that the project manager identified this as a possible risk early on in the project. She might have come across Richard Fairley's four COTS software acquisition risks (see next table), where one risk is difficulty in integrating the data formats & commn. protocols of different applications.
- She might have specified that the selected package must use a widely accepted data management system like Oracle that allows easier integration.

Fairley’s four commercial off-the-shelf (COTS) software acquisition risks

Integration	Difficulties in integrating the data formats and communication protocols of different applications.
Upgrading	When the supplier upgrades the package, the package might no longer meet the users' precise requirements. Sticking with the old version could mean losing the supplier's support for the package.
No source code	If you want to enhance the system, you might not be able to do so as you do not have access to the source code.
Supplier failures or buyouts	The supplier of the application might go out of business or be bought out by a rival supplier.

Risk mitigation

- Risk mitigation can sometimes be distinguished from risk reduction.
- Risk reduction attempts to reduce the likelihood of the risk occurring, but, risk mitigation is action taken to ensure that the impact of the risk is lessened when it occurs.
- For example, taking regular back-ups of data storage would reduce the impact of data corruption but not its likelihood. Mitigation is closely associated with contingency plans.

Risk transfer

- In this case the risk is transferred to another person or organization. With software projects, an example of this would be where a software development task is outsourced to an outside agency for a fixed fee.
- You might expect the supplier to quote a higher figure to cover the risk that the project takes longer than the average expected time.
- On the other hand, a well-established external organization might have productivity advantages as its developers are experienced in the type of development to be carried out.
- The need to compete with other software development specialists would also tend to drive prices down.

Risk Management

Contingency

- Risk reduction activities would appear to have only a small impact on reducing the probability of some risks, for example staff absence through illness.
- While some employers encourage their employees to adopt a healthy lifestyle, it remains likely that some project team members will at some point be brought down by minor illnesses such as flu. These kinds of risk need a **contingency** plan.
- This is a planned action to be carried out if the particular risk materializes. If a team member involved in urgent work were ill then the project manager might draft in another member of staff to cover that work.

Risk Management

- The preventative measures that were discussed under the 'Risk reduction' heading above will usually incur some cost regardless of the risk materializing or not.
- The cost of a contingency measure will only be incurred if the risk actually materializes.
- However, there may be some things that have to be done in order for the contingency action to be feasible.
- An obvious example is that back-ups of a database have to be taken if the contingency action when the database is corrupted is to restore it from back-ups. There would be a cost associated with taking the back-ups.

Deciding on the risk actions

- Five generic responses to a risk have been discussed above. For each actual risk, however, specific actions have to be planned. In many cases, experts have produced lists recommending practical steps to cope with the likelihood of particular risks (see, for example. Boehm's top ten software engineering risks).
- Whatever the countermeasures that are considered, they must be cost-effective. On those occasions where a risk exposure value can be calculated as a financial value using the (value of damage) x (probably occurrence) formula, the cost-effectiveness of a risk reduction action can be assessed by calculating the **risk reduction leverage (RRL).**

Deciding on the risk actions

- **RRL = (RE before – RE after)/(cost of risk reduction)**
- REbefore is the risk exposure, before risk reduction actions have been taken.
- REafter is the risk exposure after taking the risk reduction action.
- An RRL above 1.00 indicates that the reduction in risk exposure achieved by a measure is greater than its cost.

Example

- Suppose, it might cost £200,000 to replace a hardware configuration used to develop a software application. There is a 1% chance of a fire (because of the particular location of the installation). The risk exposure would be 1% of £200,000, that is £2,000.
- Installing fire alarms at a cost of £500 would reduce the chance of fire to 0.5%. The new risk exposure would be £1,000, a reduction of £1,000 on the previous exposure.
- So, RRL = (2000 – 1000)/500 = 2.0.
- Inference: The action would be deemed worthwhile.

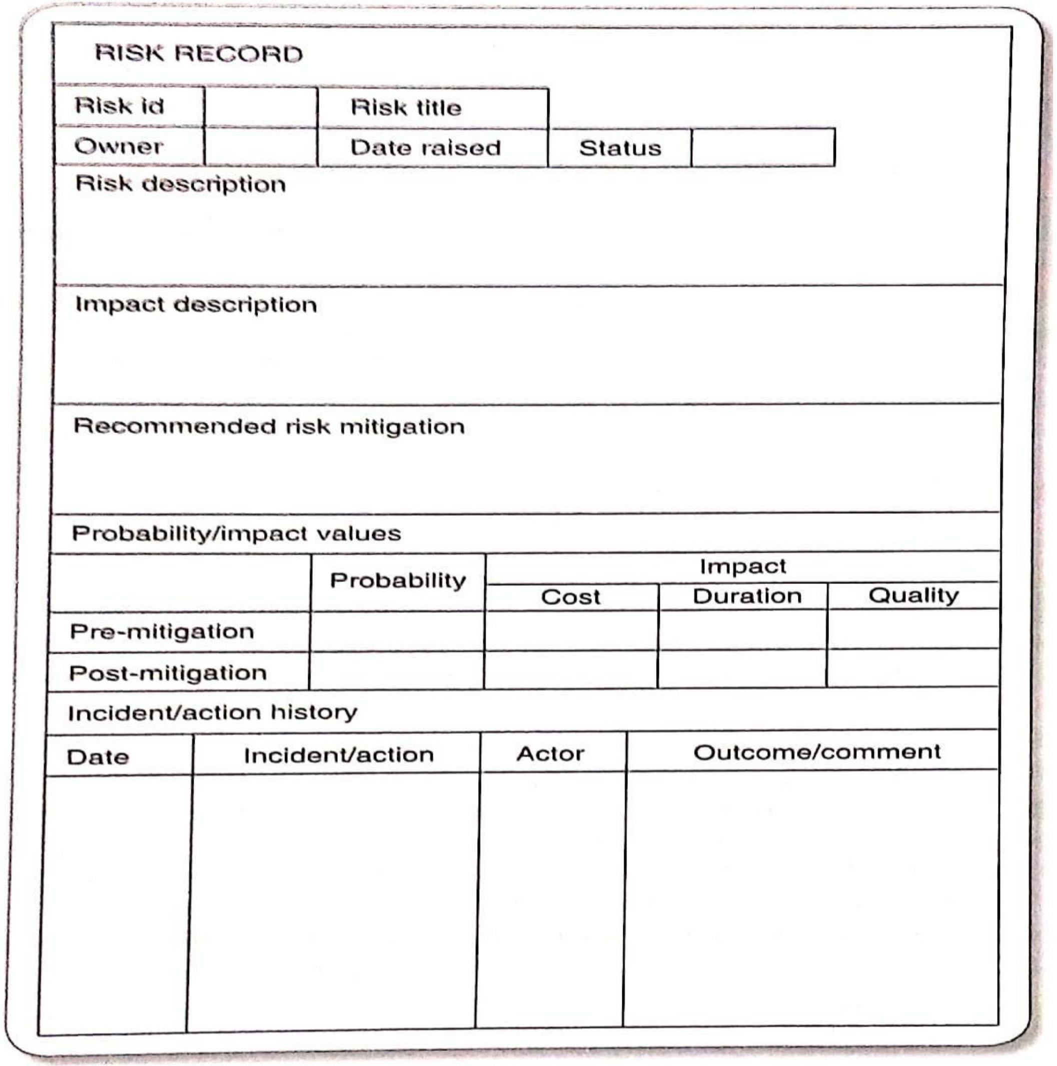
Example cont …

- Earlier, we likened risk exposure to the amount you might pay to an insurance company to cover a risk.
- To continue the analogy, an insurance company in the above example might be willing to reduce the premium you pay to have cover against fire from £2,000 to £1,000 if you installed fire alarms.
- As the fire alarms would cost you only £500 and save £1,000, the cost would clearly be worthwhile.

Creating and maintaining the risk register

- When the project planners have picked out and examined what appear to be the most threatening risks to the project, they need to record their findings in a risk register.
- After work starts on the project more risks will emerge and be added to the register. At regular intervals, the risk register should be reviewed and amended.
- Many risks threaten just one or two activities, and when the project staff have completed these, the risk can then be "closed' as no longer it is relevant.
- In any case, as noted earlier, the probability and impact of a risk are likely to change during the course of the project.

The risk register



RISK RECORD

Risk id		Risk title			
Owner		Date raised	Status		

Risk description

Impact description

Recommended risk mitigation

Probability/impact values

	Probability	Impact		
		Cost	Duration	Quality
Pre-mitigation				
Post-mitigation				

Incident/action history

Date	Incident/action	Actor	Outcome/comment

Risk Mitigation, Monitoring and Management Plan

- It is usually advisable for the project manager to develop a risk mitigation, monitoring and management (RMMM) plan for a project.
- An important component of this document is a risk table. Each row of the table contains the name of the risk, its probability and its impact on the project.
- For each risk in the risk table, the specific conditions or events that need to be monitored to check whether the risk has actually occurred is mentioned.
- The possible ways in which the risk can be avoided (mitigation) is also documented.
- A contingency plan to contain the effect of the risk is also documented.

Summary

Discussed

I. Risk identification
II. Risk analysis and prioritization
III. Risk planning
IV. Risk monitoring

References :

1. B. Hughes, M. Cotterell, R. Mall, *Software Project Management*, Sixth Edition, McGraw Hill Education (India) Pvt. Ltd., 2018.
2. R. Mall, *Fundamentals of Software Engineering*, Fifth Edition, PHI Learning Pvt. Ltd., 2018.

Thank you