© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

HOW TO MANAGE RISKS IN SOFTWARE PROJECT

Tushar Wason, Anubhav Chandra
Student, Department of Information Technology,
Dronacharya College of Engineering, Gurgaon, Hr, India

***Abstract*- Risk Management can be defined as a systematic process for identifying, analyzing and controlling risks in projects or organizations. Definitions and illustrations of risks are given especially by a list of ten risk factors, which occur most frequently in IT and Software projects. For complex, high-risk projects it is very useful to implement a formal risk-management process,supported by effective methods in the individual process steps. The importance of a sound operational preparation of each step of the risk-management process is emphasised and illustrated by examples.**

***Index Terms*- Risk Management Process, Risk, Risk Management, Identification of risks, Analysis of risks, Monitoring of risks, Project risks.**

I. INTRODUCTION

The Risk management Process is a process for proactive prevention: identifying the
things that could go wrong, assessing their impact, and determining which
potential problems need to be avoided. Risk management is an activity that must be performed by all levels of the project to ensure adequate coverage of all potential problem areas. Open communication
is required to provide all project personnel with the freedom to identify issues without negative consequences to themselves.Joint management of risks between acquirer and supplier is necessary to enable identification of the most important risks to the program and to support efficient allocation of mitigation resources. Risk management may make use of the results of other supporting processes such as Problem Resolution, Quality Assurance, and Joint Reviews.
The process consists of the following activities, to be done iteratively:

1. Risk identification
2. Risk analysis
3. Risk mitigation
4. Risk monitoring

II. THE RISK MANAGEMENT PROCESS

2.1 Risk Identification

In the risk identification step, the team systematically enumerates as many project risks as
possible to make them explicit before they become problems. There are several ways to
look at the kinds of software project risks. It is helpful to understand
the different types of risk so that a team can explore the possibilities of each of them.
Each of these types of risk is described below.
General Categories of Risk

- Generic Risks
- Product-Specific Risks
- Project Risks
- Product Risks
- Business Risks

Generic risks are potential threats to every software project. Some examples of generic
risks are changing requirements, losing key personnel, or bankruptcy of the software
company or of the customer. It is advisable for a development organization to keep a
checklist of these types of risks. Teams can then assess the extent to which these risks are
a factor for their project based upon the known set of programmers, managers, customers, and policies. Product-specific risks can be distinguished from generic risks because they
can only be identified by those with a clear understanding of the technology, the people,
and the environment of the specific product. An example of a product-specific risk is the
availability of a complex network necessary for testing. Generic and product-specific risks can be further divided into project, product, and

business risks. Project risks are those that affect the project schedule or the resources (personnel or budgets) dedicated to the project. Product risks are those that affect the quality or performance of the software being developed. Finally, business risks are those that threaten the viability of the software, such as building an excellent product no one wants or building a product that no longer fits into the overall business strategy of the company.

2.2 Risk Analysis

After risks have been identified and enumerated, the next step is risk analysis. Through risk analysis, we transform the risks that were identified into decision-making information. In turn, each risk is considered and a judgment made about the probability and the seriousness of the risk. For each risk, the team must do the following:

• Assess the probability of a loss occurring. Some risks are very likely to occur. Others are very unlikely. Establish and utilize a scale that reflects the perceived likelihood of a risk. Depending upon the degree of detail desired and/or possible, the scale can be numeric, based on a percentage scale, such as "10 percent likely to lose a key teammember" or based on categories, such as: very improbable, improbable, probable, or frequent. In the case that a categorical assignment is used, the team should establish a set numerical probability for each qualitative value (e.g. very improbable= 10 percent, improbable = 25 percent).

• Assess the impact of the loss if the loss were to occur.

Delineate the consequences of the risk, and estimate the impact of the risk on the project and the product. Similar to the probability discussion above, the team can choose to assign numerical monetary values to the magnitude of loss, such as $10,000 for a two-week delay in schedule. Alternately, categories may be used and assigned values, such as 1=negligible, 2=marginal, 3=critical, or 4=catastrophic.

Determining the probability and the magnitude of the risk can be difficult and can seem to be arbitrarily chosen. One means of determining the risk probability is for each team member to estimate each of these values individually. Then, the input of individual team members is collected in a round robin fashion and reported to the group. Sometimes the collection and reporting is done anonymously. Team members debate the logic behind the submitted estimates. The individuals then re-estimate and iterate on the estimate until assessment of risk probability and impact begins to converge. This means of converging on the probability and estimate is called the Delphi Technique (Gupta and Clarke, 1996).

The Delphi Technique is a group consensus method that is often used when the factors under consideration are subjective.

2.3 Risk Mitigation

Related to risk planning, through risk mitigation, the team develops strategies to reduce the possibility or the loss impact of a risk. Risk mitigation produces a situation in which the risk items are eliminated or otherwise resolved. These actions are documented in the Action column of the Risk Table (Table 2). Some examples of risk mitigation strategies follow:

• Risk avoidance. When a lose-lose strategy is likely (Hall, 1998)1, the team can opt to eliminate the risk An example of a risk avoidance strategy is the team opting not to develop a product or a particularly risky feature.

• Risk protection. The organization can buy insurance to cover any financial loss should the risk become a reality. Alternately, a team can employ fault-tolerance strategies, such as parallel processors, to provide reliability insurance.

Risk planning and risk mitigation actions often come with an associated cost. The team must do a cost/benefit analysis to decide whether the benefits accrued by the risk management steps outweigh the costs associated with implementing them. This calculation can involve the calculation of risk leverage (Pfleeger, 1998).

Risk Leverage =

(risk exposure before reduction – risk exposure after reduction)/cost of risk reduction
If risk leverage value, rl, is ≤ 1, clearly the benefit of applying risk reduction is not worth its cost. If rl is only slightly > 1, still the benefit is very questionable, because these computations are based on probabilistic estimates and not on actual data. Therefore, rl is usually multiplied by a risk discount factor $\rho < 1$. If ρ rl > 1, then the benefit of applying risk reduction is considered worth its cost. If the discounted leveraged valued is not high enough to justify the action, the team should look for other, less costly or more effective, reduction techniques.

2.4 Risk Monitoring

After risks are identified, analyzed, and prioritized, and actions are established, it is essential that the team regularly monitor the progress of the product and the resolution of the risk items, taking corrective action when necessary. This monitoring can be done as part of the team project management activities or via explicit risk management activities.
Often teams regularly monitor their "Top 10 risks."
Risks need to be revisited at regular intervals for the team to reevaluate each risk to determine when new circumstances caused its probability and/or impact to change. At each interval, some risks may be added to the list and others taken away. Risks need to be reprioritized to see which are moved "above the line" and need to have action plans and which move "below the line" and no longer need action plans. A key to successful risk management is that proactive actions are owned by individuals and are monitored.
(Larman, 2004)
As time passes and more is learned about the project, the information gained over time may alter the risk profile considerably. Additionally, time may make it possible to refine the risk into a set of more detailed risks. These refined risks may be easier to mitigate, monitor, and manage.

REFERENCE

[1] http://agile.csc.ncsu.edu/SEMaterials/RiskManagement.pdf
[2] http://en.wikipedia.org/wiki/Identifying_and_Managing_Project_Risk
[3] http://archive.oredev.org/download/18.5bd7fa0510edb4a8ce4800019064/1385353971845/Hns_Schaefer_-_Workshop_Risk_Based_Testing_3.pdf