Risk Analysis in Software Systems

Varsha Mittal[1] , Neena Gupta[2],

,

[1]Dept. of Computer Science & Engineering, Graphic Era University, Dehradun,India
[2]Dept. of Computer Science, Kanya Gurukula Campus, Dehradun,India

[*]*Corresponding Author: var.aadi@gmail.com   Tel.: +00-9634435387*

Abstract— Risk Identification is one of the important issues in software development.Currently, software is becoming a major part of enterprise business. Software development is activity connected with advanced technology and high level of knowledge. Risks on software development projects must be successfully mitigated to produce successful software systems. Lack of a defined approach to risk management is one of the common causes for project failures. To improve project chances for success, this work investigates common risk impact areas to perceive a foundation that can be used to define a common approach to software risk management. Based on typical risk impact areas on software development projects, we propose three risk management strategies suitable for a broad area of enterprises and software development projects with different amounts of connected risks. Proposed strategies define activities that should be performed for successful risk management, the one that will enable software development projects to perceive risks as soon as possible and to solve problems connected with risk materialization. We also propose a risk-based approach to software development planning and risk management as attempts to address and retire the highest impact risks as early as possible in the development process.

Keywords—Risk Management, Risk analysis, Risk priportization

I. INTRODUCTION

"Business people need to understand the psychology of risks more than the mathematics of risks" –Paul Gibbons
A risk is the likeliness of gaining or losing something that holds a certain value. Risks are vital and crucial for software development. "The possibility of suffering loss that describes the impact on the project which could be in the form of poor quality of software solution, increased costs, failure, or delayed completion" is described as RISK [1].
It is a well-known fact that every project shares a possibility of a considerable amount of risk which, however, can be minimized, sustained and dealt with in consonance with efficient analysis, assessment and planning. Moreover identification of the factors which can obstruct the project to be a successful product and from achieving the desired result is very crucial. Such factors are also called as Risk Factors. The cost, product quality and the duration of the project is adversely affected if these factors are not taken into consideration [2].
     The task of interpreting, elucidating and hence, examining potential risks of a project to clients is known as Risk Analysis. It also reveals the relationship between the identified risk factors and the expected outcome of the project. Risk analysis and planning goes parallel and provides an effective way of Risk control[3,4].
Risk analysis is accomplished to achieve the following objectives:

a) Curtailing threats on high level estimation of risks with all stakeholders and collaborators of the project.
b) Creating a methodical approach towards the analyzing of risks.
c) Establishing efficient risk reduction and risk removal operations.
d) Keeping track of the entire process of risk reduction.

This paper discusses the major factors of tackling risks in project management.

II. RISK MANAGEMENT STRATEGIES

Risks arise from different sources like unpredictability in economic markets, man-made or natural disturbances and disasters, perils from failure of project, political and legal liabilities etc. Aspects like project management, security, financial cases, engineering, public health etc, establish the modus operandi of risk management [5,6].
     Risk management is the process of identifying, assessing, registering and hence removing risks by applying methodical and efficient resources. It also includes all the principles and framework which are required to manage the risk effectively. The quintessence of risk management is to use the opportunities for making effective decisions to control risk that is to avoid, remove or diminish it. To control

risk, the performance board can prepare a risk assessment policy which can be evaluated at regular interval[7].

There are 4 steps under risk management. They are:

- Identification of risks
- Criteria of development assessment
- Prioritization of risks
- Response towards risks

A. *Identification of Risks*

"What could possibly go wrong in this project?" is the point of concern which requires effective solutions in this phase of risk management. It is the first and fundamental task in risk management. Identification of risk plays a key role in the success of risk management process. As an output it produces the list of risk factors that could possibly affect the performance of the project. The process of risk identification includes the following steps:

- Analysing present staff, team, methodology, employment, resources, liabilities, etc.
- Estimating potential failures.
- Analysing the negative trends.

The identified risk can be broadly categorized in two major categories:

i) Internal Risks
ii) External Risks

The table 1 shows the broad classification of the internal risks and External risks into the following categories:
Internal risks include the following categories

- i)   Product risk
- ii)   Project risk
- iii) People risk
- iv)   Process risk

B. *Development Assessment Criteria*

The first and foremost step to take while assessing risks is to develop a collective group of criteria which would be established across corporate units and projects. These risks will be assessed and examined according to their influence or probability of occurrence.

Developing Assessment Scales
It is necessary to measure risk by a particular standard, scale, or norm, without which, it becomes difficult to gauge the intensity of risks. Scales should be created in such a way which is helpful for tasks like prioritizing the risks, assessing the risks, and ranking the potency of the risks.
The rating descriptors of risks can be as follows:

Very High (5):
- No planning.
- Incapability to assess risk.
- Inefficient implementation for responses.
- Improper/ineffective crisis management modus operandi.

High (4):
- Low capability of addressing risks.
- Few emergency plans ready.
- Partial implementation.

Medium (3):
- Stress testing of risks is performed.
- Medium level capability of addressing risks.
- Most of the time, response plans are efficient and ready for implementation.
- Mostly, emergency plans are well-planned.

Low (2):
- Strategies are well defined.
- Medium-to-high level capability of addressing risks.
- Response planning is efficient and effective, except for only extreme conditions.
- Crisis management is almost perfect.

Very Low (1):
- Real-time strategies deployed.
- High-level addressed to risks.
- Response plans in place and regularly tested.
- Crisis management is perfect.

The first and foremost step to take while assessing risks is to develop a collective group of criteria which would be established

C. *Prioritization of Risks*

Comparison of risks with other risks according to their level of intensity is a procedure which can be termed as prioritization of risks. Criterion to judge risks could range from vulnerability, impact on safety and onset speed, to health factors.
After their assessment, these risks are documented into certain portfolios in order to be reported to all participants of the project.

D. *Responding To Risks*

The results of risk assessment are the inputs of risk responses, and therefore, appropriate risk strategies are developed.
They are:

- Avoidance Strategies
- Minimization Strategies

- Emergency Plans and Strategies

III.   FRAMEWORK OF RISK MANAGEMENT

The amalgamation and consolidation of all the techniques of assessing risks in accordance with the organization's governance, planning and strategizing, and managing, constitutes the structure of risk management[8,9,10].

Risk management is an extremely important task in order to generate the best quality software. It basically creates a balance between the identified risk and the methodologies to reduce the risk. The main focus in risk management is to assess the risk and develop suitable response to reduce and handle the risk[11,12]. It amplifies the better understanding of the positive aspects and negative aspects of the factors that can affect the success of the software. Efficient risk management frameworks enhance the success probability and reduce the probability of failure and uncertainty. It involves a series of 5 steps, which are:

- Establishing the context
- Identifying the risk
- Analysing the risk
- Evaluating the risk
- Treating the risk

A.   Establishing the Context

One can establish the context of the project by identifying and analyzing the objectives of the project and henceforth considering internal and external limitations within which we can manage the risks. Risk management is always done with an objective so it is considered in operational and Strategic context.

Process of establishing context:

- *Setting the scope of the assessment of risk by establishing what needs to be assessed*- It is to be identified what is to assessed. Is it software, a component or the entire project?

- *Defining broad objectives or the reasons for the assessment of risk*- The reason for risk assessment, is it a modification due to some change in policies or some operational change?

- *Identifying pertinent collaborators*- The stakeholders in risk assessment and the role of each should be clearly identified.

- *Gathering background information like strategies, audit and site reports, staff personal experiences and knowledge, expert judgment, surveys, discussions etc*- It is quite essential to have relevant information from the reliable sources for the effective risk assessment.

B.   Identifying the Risk

Identifying the risk include the identification of risk universe. Risk Universe embraces the list of all probable risk. After identifying all the probable risk they can be categorized into core and Noncore risk. Core risks are those risk which directly affect the performance of the system whereas Noncore risks are not important and be removed completely. Sources of the risk, their particular effects, and impacts, their roots and their results need to be identified on consideration of the following questions:

- *What/How/Where/Why would the risk occur?*-It refers to the identification of the reason, threats, the effected events, the outcome or consequence of the risk.

- *What will its impact be on the organization?* - The impact of risk is evaluated. Is it effecting the entire organization or its impact is local. The vicinity of risk includes- the impact on people, impact on the reputation-positive or negative for completing objective or not.

- *Who influences the project?* - The factors that influences the project like budget, resources or partners is identified it is necessary at the time of risk treatment.

C.   Analysing the Risk

After identification of the potential risks and the context, we need to analyze the pros and cons of the current modus operandi of fighting the risks. The existing controls are checked for their weakness, strength and effectiveness in handling the risk. The further actions are also identified. Process of analysing the risk:

- *Identify the existing methodologies and techniques to sort out the risk*- The current controls are evaluated for their strength to alleviate the risk. It may include the policies, functional or non-functional barriers.

- *Assessment of the likeliness of the occurrence of the risk*- Rare, possible, certain or unlikely are the likelihood of the occurrence of risk.

- *Assessment of the consequences of the risks*- The consequence or effect of risk can be moderate, minor, major, significant or insignificant

D.   Analysing the Risk

After identification of the potential risks and the context, we need to analyse the pros and cons of the current modus operandi of fighting the risks. The existing controls are checked for their weakness, strength and effectiveness in handling the risk. The further actions are also identified. Process of analysing the risk:

- *Identify the existing methodologies and techniques to sort out the risk*- The current controls are evaluated for their

strength to alleviate the risk. It may include the policies, functional or nonfunctional barriers.

- *Assessment of the likeliness of the occurrence of the risk-* Rare, possible, certain or unlikely are the likelihood of the occurrence of risk.
- *Assessment of the consequences of the risks-* The consequence or affect of risk can be moderate, minor, major, significant or insignificant.

E. Evaluating the Risk

Deciding whether the risks are acceptable or not, and how to further proceed with the risks, it all depends on the organization's willingness to bear with the risks and its consequences, considering the following circumstances:

- *Unavailability of treatment of risks-* A risk is considered to be acceptable if no treatment is available or it is decided not to treat it. But acceptable risk does not mean that it is insignificant and still need to be scrutinized.
- *Restrictive funds for treatment of risk-* The exorbitant treatment cost of risk do not encourage the treatment plan of risk especially when the risk are low ranked.
- Risk measure is low.
- Opportunities are significantly greater than the risks and threats involved.

F. Treating the Risk

Effective and constructive techniques and methodologies should be established in order to reduce the rate of occurrence and the extremity of the risk. Feasible and reliable techniques must be developed to control these threats.
Process of risk treatment:

- *Determining if a particular treatment is necessary, or if the risk could be treated with traditional methodologies-* It is to be determined if the risk can be treated with typical methods which are included in the day-to-day activity or the control for risk treatment has to be developed or modified separately .
- *Analyze and establish the type of treatment that is required for the risk-* There is a need to find out what should be the objective of the risk treatment, whether the risk can be avoided or its likeliness is to be reduced or accept the risk. The identification of the risk treatment objective will create the tolerance of the risk.
- *Design your treatment plan, keeping in mind the goal of the treatment, whether it is to reduce the impact or the frequency or the possibility of the risk-* If the objective of risk treatment is to reduce its impact or likeliness the reason for risk is identified change the approach to

mitigate the impact of risk. If the risk is to be accepted due to its low likelihood or the cost of the control development then proper documentation is maintained for future reference.

- *Lastly, ensure to evaluate your risk treatment plans and evaluate their practicality and hence, document your plan effectively-* Once the objective of the risk treatment is identified and a risk treatment plan is ready, its action, responsibilities and budget are to be reviewed accordingly.

IV. CONCLUSION

Risks can be defined as unforeseen, unpredictable events which can wreck the running of a software project. Discussing the 4 ps of project management, we assessed and analysed various risk tackling techniques and responses accordingly.

REFERENCES

[1] Hall, E. (1998): *Managing Risk: Methods for Software System Development,* Addison-Wesley, New York
[2] Jones, C. (1994): *Assessment and Control of Software Risk,* Prentice-Hall, New York
[3] Sertić, H. (2002): *Applying Unified process on complex software system development,* Master Thesis, Economic Faculty, University of Zagreb, Zagreb
[4] Booch, G.; Rambaugh, J.; Jacobson, I. (2001): *The Unified Software Development Process,* Addison-Wesley, New York
[5] Karolak, W. (1995): *Software Engineering Risk Management,* Wiley-IEEE Press, San Francisco
[6] Royce, W. (1998): *Software Project Management: A unified framework,* Addison-Wesley, New York
[7] Larman, C. (2002): *Applying UML and Patterns,* Prentice Hall, Upper Saddle River
[8] Robertson, S.; Robertson J. (2001): *Mastering the Requirements Process,* Addison-Wesley, New York
[9] Capers, J. (1994): *Assessment and Control of Software Risks,* Prentice Hall PTR, Upper Saddle River NJ
[10] Ould, M. (1996): *Strategies for Software Engineering: The Management of Risk and Quality,* John Wiley & Sons, San Francisco
[11] Charette, R. (1989): *Software Engineering Risk Analysis and Management,* McGraw Hill, New York
[12] Ould, M. (1998): *Managing Software Quality and Business Risk,* John Wiley & Sons, San Francisco