International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Models, Techniques and Metrics for Managing Risk in Software Engineering

Er. Jaspreet Kaur

Abstract –*Researchers in software industry have focused on risk management for long time. Software Risk management is a practice that embodies risk identification, risk estimation, mitigation, and monitoring which delivers a disciplined environment for efficient decision making to evaluate the problems in software development. In large-scale system, measurement of risk is comparatively difficult because of its complex nature[4]. Moreover, large-scale systems are challenging since many risks can arise during system development. In this paper, tools are further divided into subcategories according to those that are best suited. Comparative analysis is presented in this paper for different software related risk management models with some commonly identified features and further categorize them into classes based on the severity of the risk. A brief introduction is also provided to understand the concepts of risk management for software development projects, and overview of risk management framework.*

Key Words: Risk Management, Risk Factors, Risk Exposure, Risk Estimation, Mitigation and Metrics

1. INTRODUCTION

Statistics indicate that more than 53% of software development projects have been behind budget and schedule and are unable to deliver features originally specified; 31% of development projects are ended in premature cancelling or termination and around 61% of them are able to satisfy original specified requirement features. Hence, the project management associates itself with plan and management of resources or any type of changes in an organization in any dimension. Dimensions are staffing, products, people and services, production and distribution, budgeting, financing, purchasing, marketing, selling, human resources training and development or anything else which requires planning as well as management. The risk inherited in projects is required to be managed early in the SDLC model and testing of software is done based on risk identified and analyzed[3]. The software testing also needs selective and careful planning as software Testing is not performed exhaustively. In case of risky scenarios, proper identification of risky items is needed as there are quite restricted resources and shortage of time. If early predictions about risk in software testing are done on time, software quality is improved. Software testing and Risk management is joint together to solve two type of issues. Testing is mainly required to support the software risk management process and risk management to support software testing.

2. RISK MANAGEMENT TOOLS

Risk can cause extensive losses and threats for various organizational procedures. In Computer Science engineering, risks can come from networks, the Internet, malicious codes or users, loopholes and from physical security. There are many types of risks that may occur while creating high quality software systems that cannot be completely eliminated but project managers can reduce their impact on products by calculating these risks on IT resources. Software systems have become more complex and are known to be large-scale systems in current era. Complexity and Increases in project size result in increases of various risks. According to surveys, every year an average of $350 billion of off-the-shelf software are sold. In case of large-scale systems, risk management is an investment that can be valuable in the future because of high quality and reliability demands. The goal behind risk management system is to identify and control all possible risks before they occur during software development. Risk can be classified as systematic risks and unsystematic risks.[2] The risks caused by external factors, including hacking, viruses, natural disasters and power loss are known as Systematic Risks. For example systematic risk is vulnerable browser, in which any kind of loophole may lead to security breaches and can harm the resources of that organization whereas unsystematic risks cause unique risks for the firm, including the misuse of confidential data, application error, inside attacks, data loss, equipment malfunctions and human interactions. Systematic risks are also known as generic risks whereas unsystematic risks are known as specific risks. Classification of risks in software development is described in Figure 1. The task of Risk management team is to continually assess and monitors various risks and determines their negative impacts on software development. Risk management systems provide a dynamic way for decision-making by prioritizing and ranking the risks. Normally, a risk management system is based on the identification and assessment of risks.

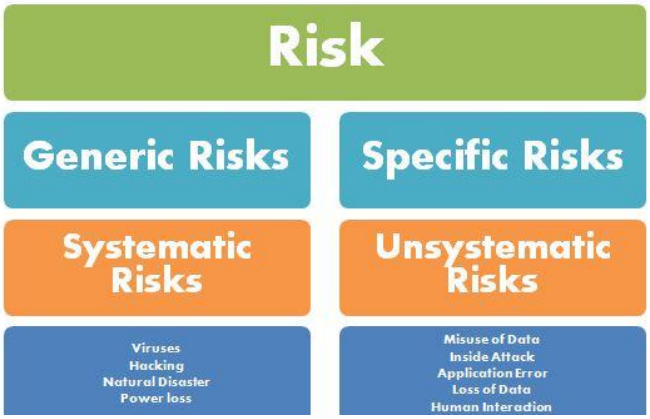

Fig -1: Types of Risks in Software Development

Like many other businesses, software development risk cannot be eliminated, but risk managers can reduce the impact of these risks by using appropriate risk management tools and techniques. The risk management process requires tools that can identify and be applied to perceived risks. Through analyzing the existing literature of risk management in software development, we have listed and categorized some risk management tools that are considered to be helpful for mitigating risks.

3. SOFTWARE RISK MANAGEMENT PROCESS

Risk management focuses on identifying and assessing the risks to the project and managing those risks to minimize the impact on the project[2]. There are no risk-free projects because there are infinite numbers of events that can have a negative effect on the project. Risk management is not about eliminating risk but about identifying, assessing, and managing risk. Risk management means risk containment and mitigation. First, we have to identify and plan. Then be ready to act when a risk arises, drawing upon the experience and knowledge of the entire team to minimize the impact to the project.

Risk Management as shown in Figure 2, comprises of following processes:

- Identify the Risk: Recognize and describe risks that might affect successful implementation of the systems.
- Analyze the risk: Once risks are identified, determine the likelihood and consequence of each risk.
- Evaluate or Rank the Risk: Evaluate or rank the risk by determining the risk magnitude, which is the combination of likelihood and consequence. We need to make decisions about whether the risk is acceptable or whether it is serious enough to warrant immediate action.
- Treat the Risk: This is also referred to as Risk Response Planning. During this step assess highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels.
- Monitor and Review the risk: This is the step used to monitor, track and review risks.
- Communicate risk status throughout project

Fig -2: Risk Management Process

4. RISK CATEGORIES

Risks are identified, classified and managed before starting the actual development of a system. These risks are classified in different categories.

A. Schedule Risk

- Project schedule get slip when project tasks and schedule release risks are not addressed properly. Schedule risks mainly affect on project and finally on company economy and may lead to project failure. Schedules often slip due to following reasons:
- Wrong time estimation
- Resources are not tracked properly. All resources like staff, systems, skills of individuals etc.
- Failure to identify complex functionalities and time required to develop those functionalities.
- Unexpected project scope expansions.

B. Budget Risk

- Wrong budget estimation
- Cost overruns
- Project scope expansion.

C. Operational Risks

Risks of loss caused due to improper process implementation, failed system or some external events risks.

Causes of Operational risks:

- Failure to address priority conflicts
- Failure to resolve the responsibilities
- Insufficient resources
- No proper subject training
- No resource planning
- No communication in team.

D. Technical Risks

Technical risks generally lead to failure of functionality and performance.

Causes of technical risks are:

- Continuous changing requirements
- No advanced technology available or the existing technology is in initial stages.
- Product is complex to implement.
- Difficult project modules integration.

E. Programmatic Risks

These are the external risks beyond the operational limits. These are all uncertain risks are outside the control of the program.

These external events can be:

- Running out of fund.
- Market development
- Changing customer product strategy and priority
- Government rule changes.

4. TOOLS AND TECHNIQUES FOR RISK MANAGEMENT

Risk Assessment tools are important for any software projects to be delivered successfully. It is a regulatory requirement in some organization for quality audit and compliance process. An automated Risk Assessment tools reduces audit time and findings, and a decreases risk of project failure. It improves product quality, increases customer satisfaction, and ensures the requirements are implemented in full with compliance acceptance[1].

There are six major risk management process has been elaborated with its Inputs, Tools, Techniques and Outputs.

- Plan Risk Management
- Risk Identifications
- Qualitative Risk Analysis
- Quantitative Risk Analysis
- Plan Risk Responses
- Control Risks

4.1 Plan Risk Management

Risk management planning is the process of deciding how to approach and plan the risk management activities for a project. It is important to plan the risk management processes that follow to ensure that the level, type, and visibility of risk management are commensurate with both the risk and importance of the project to the organization[1].

Inputs	Tools and Techniques	Output
• Risk Management Plan • Cost Management Plan • Schedule Management Plan • Quality Management Plan • Human resource Management Plan • Scope baseline • Activity Cost estimates • Activity Duration estimates • Stakeholder register • Project documents • Procurement documents • Enterprise environment factors • Organizational process Assets	• Documentation reviews • Information gathering techniques • Checklist analysis • Assumptions analysis • Diagramming analysis • SWOT analysis • Expert judgement	Risk Register

Table 1: Risk Identification Process

4.2 Qualitative Risk Analysis

Prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact. Qualitative risk analysis includes methods for prioritizing the identified risks for further action, such as risk response[1]. The risk management can improve the project's performance effectively by focusing on high priority risks.

Inputs	Tools and Techniques	Output
• Risk Management Plan • Scope baselines • Risk Register • Enterprise environmental factors • Organizational process assets	• Risk probability and impact assessment • Probability and impact matrix • Risk data quality assessment • Risk categorization • Risk urgency assessment • Expert judgment	Project document updates

Table 2: Qualitative Risk Analysis

4.3 Quantitative Risk Analysis

Numerically analyzing the effect of identified risks on overall project objectives. Quantitative risk analysis goes at least one stage further than qualitative analysis by attempting to quantify the outcome of a risk event or to attach a numerical score to the risk according to its perceived claim for preventive or mitigating action. Quantitative analysis methods attempt to assign numerical values to risks and their possible effects[1]. They often examine the probable impact on project time and costs. Alternatively, the evaluation process can produce a ranking number for every identified risk. Ranking numbers denote the priority that a risk should claim for management attention and expenditure on preventative measures.

Inputs	Tools and Techniques	Output
Risk management plan Cost management plan Schedule management plan Risk register Enterprise environment factors Organizational process assets	Data gathering and representation techniques Quantitative risk analysis and modeling techniques Expert judgment	Project document updates

Table 3: Quantitative Risk Analysis

4.4 Plan Risk Responses

Developing options and actions to enhance opportunities and reduce threats to project objectives.

1) Plan Risk Responses Definitions

- Risk Trigger: A sign which provides warning that risk is about to occur
- Contingency Plan: Planned response to be performed when trigger happened
- Fallback Plan: Plan to be used when planned response prove ineffective
- Residual Risk: Risk remains after acceptance
- Secondary Risk: A direct result of implementing a risk response
- Workaround: Unplanned response developed to deal with occurrence of unanticipated risk events
- Contingency Reserve: Funds or time allocated by PM for known-unknowns
- Management Reserve: Funds or time allocated by top management for unknown-unknowns.

Inputs	Tools and Techniques	Output
• Risk management plan • Risk register	• Strategies for negative risk or threats • Strategies for positive risks or opportunities • Contingent response strategy • Expert judgment	Project management plan updates Project document updates Risk register updates.

Table 4: Plan Risk Responses

4.5Control Risks

Implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness throughout the project.

Monitor & Control Risk

- Tracking existing risks
- Look for occurrence of risk triggers
- Monitor residual risks
- Evaluate effectiveness of risk management plan

- Collect / communicate risk status
- Determine if assumptions still valid
- Implementing risk response plans (using the Plan risk responses process)
- Recommend corrective actions

Use contingency reserves Risk Reassessment Periodically review risk management plan and risk register and adjust them as required

- Also, close risks that are outdated
- Risk Audit Auditors should ask the project team to prove that they have identified all the risks, have plans for each major risk, and risk owner is prepared to take action.
- Evaluating risk process effectiveness continuously

Inputs	Tools and Techniques	Output
• Project management plan • Risk register • Work performance data • Work performance reports	• Risk reassessment • Risk audits • Variance and trend analysis • Technical performance measurement • Reserve analysis • Status meetings	• Work performance information • Change requests • Project management plan updates • Project document updates • Organizational process assets updates

Table 4: Control Risks

5. COMMONLY USED TOOLS FOR RISK MANAGEMENT

The risk register lists all the risks identified at the beginning and during the life of the project, their grading in terms of likelihood of occurring and seriousness of impact on the project, initial plans for mitigating each high level risk, and subsequent results.

It usually includes:

- A unique identifier for each risk
- A description of each risk and how it will affect the project
- An assessment of the likelihood it will occur and the possible seriousness/impact if it does occur (low, medium, high)
- A grading of each risk according to a risk assessment table
- An outline of proposed mitigation actions (preventative and contingency).

The register should be maintained throughout the project and will change regularly as existing risks are re-graded in the light of the effectiveness of the mitigation strategy, and new risks are identified. In smaller projects, the risk register is often used as the risk management plan[5].

6. CONCLUSIONS

In this way, software risk management, risks classification, and strategies for risk management are clearly described in this paper. If risk management process is in place for each and every software development process then future problems could be minimized or completely eradicated. Risk management is an extensive discipline, and we have given only an overview here. The best practices or summary of managing risk on software development and software engineering projects:

- Always be forward thinking about risk management. Otherwise, the project team will be driven from one crisis to the next.
- Use checklists, and compare with similar previous projects.
- Risks, ranking each according to the severity of exposure.
- Develop a top-10 or top-20 risk list for the project.
- Vigorously watch for surfacing risks by meeting with key.
- As practicable, split larger risks into smaller, easily recognizable and readily-manageable risks.
- Strongly encourage stakeholders to think proactively and communicate about risks throughout the entire project.

Understanding various factors Prioritize under risk management process and focusing on risk management strategies explained above could help in building risk free products in future.

REFERENCES

[1] K.Adalarasan and Dr.R.Balu, “A Narrative Study on Design and Development of Risk Management Tools for Software Development,” vol. 4, July 2016.

[2] Raghavi Bujhang, “Recent Trends of Risk Management in Software Development: An Analysis,” July 2018.

[3] Bibash Roy,"A study of Software Risk Management Strategies and Mapping with SDLC,"May 2015.

[4] Marfuf Pasha, Ghazia Qaiser and Urooj Pasha," A Critical Analysis of Software Risk ManagementTechniques in Large Scale Systems" December 2017.

[5] Anand Kumar Roy, Dr. Shalini Agrawal2,Dr. MazaharKhaliq,"Identification of Agile Software Risk Indicators and Evaluation of Aglie Development Project Risk Occurance Probability", July 2017.

[6] Mumtaz Ahmad Khan, Shadab Khan, Mohd Sadiq, "Systematic Review of Software Risk Assessment and Estimation Models", April 2012.

BIOGRAPHIES

Er Jaspreet Kaur received Bachelor Degree in Computer Science & Engineering and Mater Degree in Information Technology. Worked as Assistant Professor in various colleges with experience more than 10 years in Teaching in CSE/IT Department.