International Journal of Research (IJR) Vol-1, Issue-9, October 2014 **ISSN 2348-6848**

Software Risk Management and Risk Mitigation Technique

Kunal Deswal[1]& Shweta Thakur[2]

Student, Dept. of Information Technology. DCE, Gurgaon, Harayana, India

ABSTRACT

Software Engineering is the craft of creating the software in a fitting way by utilizing the software development life cycle. The advancement in software technology is an element movement and obliges a considerable measure of sensible speculation amid this methodology. The objective of this paper is to clarify the idea of risk and to create its part inside the software development process. Additionally to present the utilization of risk management as an intend to identify and control risk in product.

Keywords-

Software Engineer;Software Development; Software Risk Management; Risk Avoidance; Software Development; Risk Mitigation.

Abbreviation- *SPM – Software Project Management; SRM – Software Risk Management; WoV- Window of vulnerability*

1. INTRODUCTION

Risk management is the methodology of recognizing risk issues and the alternatives for controlling them, appointing a risk appraisal, surveying the results and selecting amongst the evaluated choices to best meet the objectives. Software risk management has been an extremely hot range of exploration since most recent three decades. As of late, the exploration group looks genuinely intrigued to recognize the risk calculates as well as the reasons for the presence of the risk figures in software development life cycle and how these risks can either be taken care of or maintained a strategic distance from.

Fig.1. Risk management

1.1 WHAT IS RISK

Risk is the potential of loss (an undesirable outcome, however not necessarily so) resulting from a given action, activity and/or inaction. The notion implies that a choice having an influence on the outcome sometimes exists (or existed). Potential losses themselves may also be called "risks". Any human endeavor carries some risk, but some are much riskier than others.

1.2 DEALING WITH RISK

The right method to deal with a risk is to identify it first. Once the risk is identified, analyse its implication and determine treatment methods. The next step involves monitoring the performance of treatment methods, techniques and heuristics for the identification, analysis, treatment and monitoring of risk. Risk management is a project management tool to assess and mitigate events that might adversely impact a project, thereby increasing the likelihood of success.

1.3 WHY IS SOFTWARE WORLD INTRESTED IN RISK?

Numerous post-mortems of software project disasters show that issues would have been stayed away from (or strongly reduced) if there had been an express early concern with distinguishing and determining high-risk components. A clear variable!

2. SOFTWARE RISK MANAGEMENT

Software risk management is a software building practice with techniques, systems, and tools for overseeing risks in a task or project. It gives a restrained environment to proactive choice making to evaluate ceaselessly what can happen; figure out what risks are paramount to manage; and execute activities to manage those risks. Risk management arranging addresses the technique for risk management, the risk management process, and the methods, routines, and apparatuses to be utilized to help the risk management process.

2.1 ROLE OF MANAGEMENT

Senior management backing and duty is critical to the accomplishment of any risk management activity. A formal risk management procedure requires corporate acknowledgement of risk as a significant consideration for software management.

Senior management must support project risk management activities by: (1) providing adequate personnel, budget, schedules, and other resources (e.g., tools and equipment); (2) ensuring project management receives the required training in identifying, managing, and communicating software risks; and (3) ensuring project personnel receive the required training in conducting risk management tasks. Senior management reviews risk management activities on a periodic and event-driven basis.

3. SOFTWARE RISK MANAGEMENT PROCESS

Risk is any anticipated unfavorable event that occur while the project is underway and risk management means reducing the impact of all kinds of risks that might affect a project.

3.1 PROCESS MODEL

There are a few models accessible for risk management. This model may be custom-made to be predictable with existing site venture management forms. In all periods of a task, risks ought to be evaluated constantly and utilized for choice making. This model recognizes the central risk management works that must be taken to viably oversee risk: recognize, break down, plan, track, control, and impart.

3.2 PROCESS DESCRIPTION

Fig.2. Risk Management Overview

3.2.1 SOFTWARE RISK MANAGEMENT PROCESS: AN OVERVIEW

A review of the risk management process, alongside a mapping to the risk management model is represented in Figure.

3.2.2 SOFTWARE RISK MANAGEMENT PROCESS: SPECIAL RESPONSIBILITIES

Personnel from the software engineering staff are selected to participate on a Software Risk Evaluation (SRE) Team. An SRE Team should have from one to five participants. The following criteria should be used in selecting participants:

- risk management experience or will receive risk management training
- knowledge and experience in the technology areas of the effort being assessed

- mix of people with various applicable skills (e.g. development, test, quality assurance), and
- Representation for any functional areas considered critical to the project.

An individual is selected to serve as the facilitator for the risk management process. The SRE Facilitator should be someone who does not have a vested interest in the results of the process and can effectively move the process to closure. This person should meet the entrance criteria for this process; that is, they should have risk management experience or receive training.

3.2.3 SOFTWARE RISK MANAGEMENT PROCESS: INPUTS

Inputs are those things that must be accessible with a specific end goal to begin the risk management process. Inputs will be utilized/changed by the methodology steps into yields. Samples of inputs are:

a. Organizational standards, practices, guidelines as tailored to this project
b. Software artifacts, e.g., system/software requirements
c. Software Project Plan
d. Risk Management Plan Template
e. Risk Management Forms

3.2.4 SOFTWARE RISK MANAGEMENT PROCESS: PROCEDURES

The risk management procedure comprises of ten steps as portrayed in the passages that take after. Utilization of the exercises connected with these steps constitutes a satisfactory risk management approach and could be consolidated into a Risk Management Plan. The size, visibility, or outcomes of the venture drives the multifaceted nature of the methodology. The methodology can be customized to be consistent with existing site project management processes.

Function 1: Identify

Before risks can be managed, they must be identified, and they must be identified before they become problems adversely affecting the project. Establishing an environment that encourages people to raise concerns and issues and conducting quality reviews throughout all phases of a project are common techniques for identifying risks.

Function 2: Analyze

Analysis is the conversion of risk data into risk decision-making information. It includes reviewing, prioritizing, and selecting the most critical risks to address.

STEP 2: Analyze Risks

The SRE Team analyzes each identified risk in terms of its consequence on cost, schedule, performance, and product quality. An individual risk may impact more than one of these categories. For example, frequently changing requirements will impact all four.

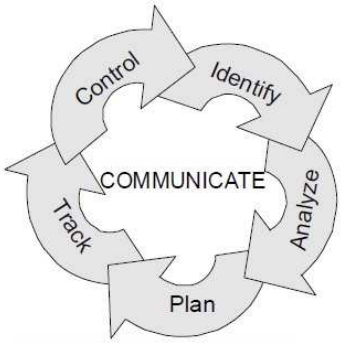
STEP 3: Prioritize Risks

Using the data from step 2, Analyze Risks, the SRE Team determines a Risk Level for each risk by mapping each risk onto a Risk Matrix. The project and risk management personnel evaluating the Risk Level for each risk can determine when appropriate mitigation action will be required. This decision making can be facilitated by the use of risk levels agreed to by the SRE Team and project management.Where the Risk Levels are defined as:
a. Tolerable Risk is a condition where risk is identified as having little or no effect or consequence on project objectives; the probability of occurrence is low enough to cause little or no concern.
b. Low Risk is a condition where risk is identified as having minor effects on project objectives; the probability of occurrence is sufficiently low to cause only minor concern.
c. Medium Risk is a condition where risk is identified as one that could possibly affect project objectives, cost, or schedule. The probability of occurrence is high enough to require close control of all contributing factors.
d. High Risk is the condition where risk is identified as having a high probability of occurrence and the consequence would affect project objectives, cost, and schedule. The probability of occurrence is high enough to require close control of all contributing factors,

the establishment of risk actions, and an acceptable fallback position.

e. INtolerable Risk is the condition where risk is identified as having a high probability of occurrence and the consequence would have significant impact on cost, schedule, and/or performance. These risks would constitute the Top N for the project.

At the conclusion of risk prioritization, a consolidated list of risks is created, and the updated Risk Management Forms are placed under configuration management.



A continuous set of activities to identify, confront, and resolve technical risk.

Identify	Search for and locate risks before they become problems adversely affecting the project
Analyze	Process risk data into decision-making information
Plan	Translate risk information into decisions and actions (both present and future) and implement those actions
Track	Monitor the risk indicators and actions taken against risks
Control	Correct for deviations from planned risk actions
Communicate	Provide visibility and feedback data internal and external to your program on current and emerging risk activities

Fig.3. Risk Management Process

Function 3: Plan

Planning turns risk information into decisions and actions for both the present and future. Planning involves developing actions to address individual risks, prioritizing risk actions and creating a Risk Management Plan. The key to risk action planning is to consider the future consequences of a decision made today. The plan for a risk can be to:

a. Mitigate the impact of the risk by reducing its Risk Level.
b. Avert a risk by changing the design or the process or by taking no further action thus accepting the consequences if the risk occurs.
c. Develop a contingency strategy should the risk occur.

STEP 4: Identify Risk Aversion Methods

Having generated a ranked list of risks, the SRE Team performs an analysis to determine what risk aversion actions (i.e., risk avoidance, control, assumption, or transfer) could be taken or decisions could be made that would eliminate any of the identified risks. The SRE Team assesses, rates, and decides on the possible consequences of inaction and if the benefits of acting on a risk merit the expense in time and money expended. While a conscious decision to ignore a high risk may be a creditable option, an unconscious decision to avoid risk is not. This step could concentrate on steady process change by recognizing those hierarchical (or venture) forms that would dispose of, or considerably diminish, a given risk. Utilizing risk management working together with measurements and procedure change can be utilized to measure, track, and enhance an association's development process.

STEP 5: Identify Risk Mitigation Methods

Risks that make it to this step are viewed as dependent upon outside occasions. A SRE Team session is held to figure out what activities or choices can be made that would decrease the likelihood and/or seriousness of effect of each one risk occasion. The SRE Team reports and points of interest those that are commonsense and practical and joins them into the undertaking Risk Management Plan. This sort of procedural detail would permit both the specialized leads and the foremen to anticipate issue zones and make fitting move to evade or minimize risk.

STEP 6: Identify Risk Recovery Methods

For each of the top N risks, the SRE group leads a session to approve the way of the occasion that would result in the summon of a possibility activity. Possibility activities for risks

are archive in the task Risk Management Plan alongside what measurable or noticeable circumstances must jump out at trigger the usage of the possibility activity.

STEP 7: Define Risk Metrics

For each risk, the SRE Team determines and documents what measurable or observable event(s) can be tracked to know whether or not the risk is being averted, prevented, or minimized. For instance, if testing has been distinguished as a high risk work then following test scope examination at unit test time and deciding blunder evacuation rates for outline audit, unit testing, and mix testing could serve as key measurements. Other conceivable test measurements could incorporate following of the delta in the middle of open and shut inconvenience reports and the following of mistake thickness by inconvenience report need. Furthermore, the SRE Team characterizes and archives the risk management process estimations to be gathered and dissected on the risk process itself. Cases are given in segment 2.2.8.

STEP 8: Implement Mitigation/Reduction Actions

For each one risk, the SRE Team leads the exercises important to actualize the relief/decrease activities tended to in step 5 above. These exercises are recorded in the task Risk Management Plan for each one risk lessening situation. Samples of exercises that would address the risk levels characterized in step 3 are:

a. Tolerable Risk. Good system engineering practices would serve to mitigate any problems of this magnitude.
b. Low Risk. No special program emphasis is required other than normal software engineering group monitoring and control.
c. Medium Risk. This risk level would qualify as an action item at status review meetings.
d. High Risk. This risk level qualifies as an action item at status review meetings.
e. Insufferable Risk. This level obliges formal control and checking and development of a risk possibility activity. Each one risk at this level has a meaning of the occasion that would summon the possibility activity. The deviation qualities are situated restricted enough to bring a risk banner up in time to permit the venture authority time to react yet open enough to not make extreme raised banners. The deviation qualities are recorded with the metric depiction.

Function 4: Track

Tracking consists of monitoring the status of risks and the actions taken against risks to mitigate them. This is done through appropriate risk metrics and serves as the "watchdog" function of risk management.

STEP 9: Track Risks

Projects implement reporting procedures that raise attention flags whenever a reported metric or parameter is beyond the pre-established monitor threshold or deviation value. The method and time of collecting and reporting each metric are incorporated into the Risk Management Plan. The RM Manager guarantees the reporting strategies of the Risk Management Plan are continuously taken after and inferred measurements are figured; gets and breaks down the reports, and takes fitting remedial activities as needed.

Function 5: Control

Risk control corrects deviations from planned risk actions. Risk control is a part of project management and relies on project management processes to control risk action plans, correct for variations from plans, respond to triggering events, and improve risk management processes. Risk control activities are documented in the Risk Management Plan.

STEP 10: Implement Contingency Actions

For each risk, if the data collected shows that the entrance criteria have been met, then:

- the need for implementation of the contingency action should to be raised to the Program Manager, and
- project management needs to provide for the direction necessary to reallocate resources required for the execution of that contingency action.

Function 6: Communicate

Communication lies at the core of the model to underline its pervasiveness and its criticality. Communication happens all through

all the capacities of risk management. Without powerful communication, no risk management methodology can be suitable. It is a vital piece of the various risk management exercises. Obviously, staff connected with a venture are the most qualified to distinguish risk in their work consistently. Venture management gives a helpful environment to individuals to impart their worries in regards to potential risks. Successful communication gives both perceivability and input information, interior and outer to your project, on present and developing risk exercises.

4. NEED TO MANAGE RISK

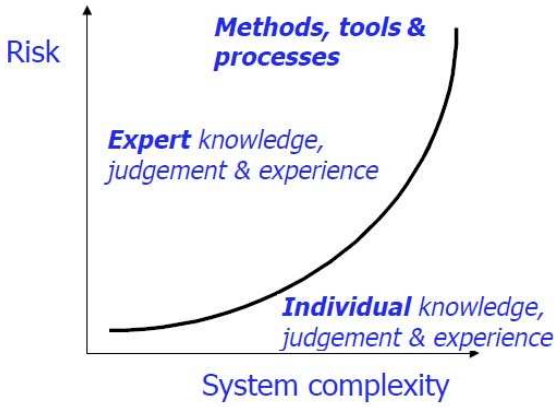


Fig.4. Need for Risk Management

5. CONCLUSION

Software Engineering is the craft of creating the software in a fitting way by utilizing the software development life cycle. The advancement in software technology is an element movement and obliges a considerable measure of sensible speculation amid this methodology. As the development of software is getting to be more precise, methodical and instrument driven, the risks are expanding and the consideration regarding risk management is not expanding with the same pace. Along these lines the scholastic and also mechanical group is worried about the risks and how they can be taken care of to minimize the misfortunes and to build the benefits and notoriety in the business. This examination article put in light the part of recommending the procedures to handle or deal with the software risks. This paper proposes tending to the risk components to be dealt with by the innovation as well as by utilizing instinct also.

12. REFERENCES

[1]. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.

[2]. Keil, M., Cule, P. E., Lyytinen, K., & Schmidt, R. C. (1998). A framework for identifying software project risks. *Communications of the ACM*, *41*(11), 76-83.

[3]. Fairley, R. (1994). Risk management for software projects. *IEEE software*, *11*(3), 57-67.

[4]. Boehm, B. W., & DeMarco, T. (1997). Software risk management. *IEEE software*, *14*(3), 17-19.

[5]. Higuera, R. P., & Haimes, Y. Y. (1996). *Software Risk Management* (No. CMU/SEI-96-TR-012). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.