



**RESEARCH ARTICLE**

# Software Risk Management

P. M. Chawan<sup>1</sup>, Jijnasa Patil<sup>2</sup>, Radhika Naik<sup>3</sup>

<sup>1</sup>Department of Computer Technology, Veermata Jijabai Technological Institute Matunga, Mumbai, India

<sup>2</sup>Department of Computer Technology, Veermata Jijabai Technological Institute Matunga, Mumbai, India

<sup>3</sup>Department of Computer Technology, Veermata Jijabai Technological Institute Matunga, Mumbai, India

<sup>1</sup> [pmchawan@vjti.org.in](mailto:pmchawan@vjti.org.in); <sup>2</sup> [jijnasa.patil@gmail.com](mailto:jijnasa.patil@gmail.com); <sup>3</sup> [radhika.u.naik@gmail.com](mailto:radhika.u.naik@gmail.com)

---

**Abstract**— *Software Risk Management is a critical area among the nine knowledge areas used in Software project management. This paper describes different frameworks and paradigms used in risk management. A framework or a model is decided for managing risks in a project. This model acts as a tool for efficient risk management. It has basic steps of Risk identification, risk planning, risk assessment, risk mitigation and risk monitoring and controlling.*

**Key Terms:** - *Framework; risk management*

---

## I. INTRODUCTION

Nowadays, project management has become a part and parcel of all organizations. To accomplish any project successfully, it is necessary to plan and manage all activities of the project. One of the most important aspects of IT projects is risk. Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). 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 more risky than others. This definition of risk promotes the negative aspect of risk alone. In case of IT or software projects, there are also positive risks and opportunities. A project risk therefore is an uncertainty that can have a negative or positive effect on meeting project objectives. Risk project management involves identification, assessment and monitoring and control of possible risks involved in the project. There should be a balance between risks and opportunities. The software project risk in IT industry refers to the questions in such aspects as budget and progress encountered in the software development course and the impacts of the questions on software project. The project risk of the software may affect the realization of the project plan, and if the project risk turns into reality, it will affect the progress of the project and increase the cost of the project, even make the software project unfeasible. The software project development is an activity that can leads to loss. No matter how to implement the course of development, over budget and delay happens regularly. The developing mode of project can't guarantee the ultimate success. We have to take a risk in project development and analysis the project risk. While carrying on the risk analysis of the project, attention must be paid to measure the degree of uncertainty and the equivalent loss degree of each risk. The goal of project risk management is minimizing potential negative risks while maximizing potential positive risks.

Risk can be categorized as: [1][2]

1. Known risks: the risks that can be found after assessing the project plan, the commercial and technological environment and other reliable informational sources carefully (for example: unrealistic delivery time, no demand, software file and abominable developing environment)

2. Unknown risks: perhaps they will appear really, but it is very difficult to recognize them coming in advance.
3. Predicted risks: it can be inferred from the previous experience (for example: Personnel adjustment, no communication with customers, making developer's energy dispersed because of maintaining).

A software project may encounter various types of risks: [3]

- Technical risks include problems with languages, project size, project functionality, platforms, methods, standards, or processes. These risks may result from excessive constraints, lack of experience, poorly defined parameters, or dependencies on organizations outside the direct control of the project team.
- Management risks include lack of planning, lack of management experience and training, communications problems, organizational issues, lack of authority, and control problems.
- Financial risks include cash flow, capital and budgetary issues, and return on investment constraints.
- Contractual and legal risks include changing requirements, market-driven schedules, health & safety issues, government regulation, and product warranty issues.
- Personnel risks include staffing lags, experience and training problems, ethical and moral issues, staff conflicts, and productivity issues.

Other resource risks include unavailability or late delivery of equipment & supplies, inadequate tools, inadequate facilities, distributed locations, unavailability of computer resources, and slow response times.

## II. RISK MANAGEMENT MODELS

### A. SRE's Project Risk Management Paradigm

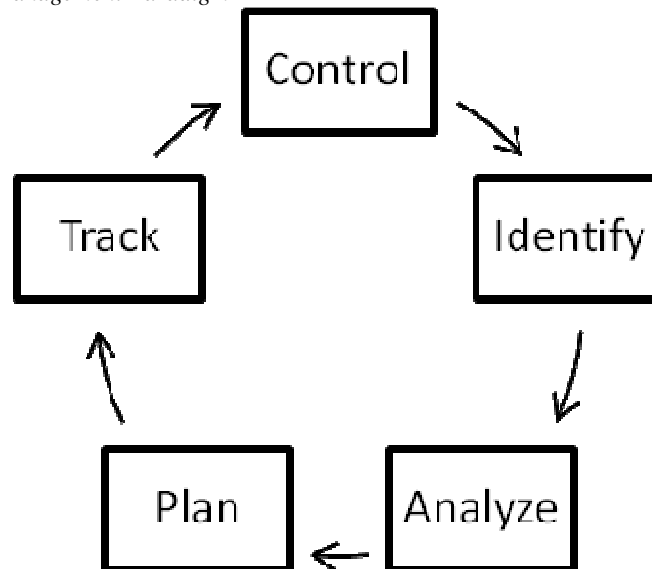


Figure 1: SRE's Project Risk Management Paradigm

There are several models available for risk management. The model developed by the Software Engineering Institute (SEI) [4][5] is shown in Figure 1. This approach concentrate on all the risk areas in the project in form of a classification based questionnaires. SRE is not only a diagnostic but also decision-making tool for a project. This technique deals with risks from product, process and constraints. It identifies those risks and categorizes project risk statement. SRE provides clear and understandable picture of the risks of the project. It diagnosis the risks and decide whether there any risk acceptable for starting a project or not. To identify risks before they become threat for project, SRE creates risk baseline. It can also reset risks baseline for the project. It works accordingly SEI standard and addresses the identification, analysis, planning, and communication elements of the SEI (Software Engineering Institute) Risk Paradigm. The analysis risk element is also covered fully by SRE activities. In SRE, construction of high-level mitigation strategy plans partially address planning element. The SRE also contributes significantly to the communication element. [4][5]

**Identify:** Before risks can be managed its must be identified before 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.

**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. The Software Risk Evaluation (SRE) Team analyzes each identified risk in terms of its consequence on cost, schedule, performance, and product quality.

**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.

**Track:** Tracking consists of monitoring the status of risks and the actions taken against risks to mitigate them.

**Control:** Risk control 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.

**Communicate:** Communication happens throughout all the functions of risk management. Without effective communication, no risk management approach can be viable. It is an integral part of all the other risk management activities.

### B. Team Risk Management Process Set

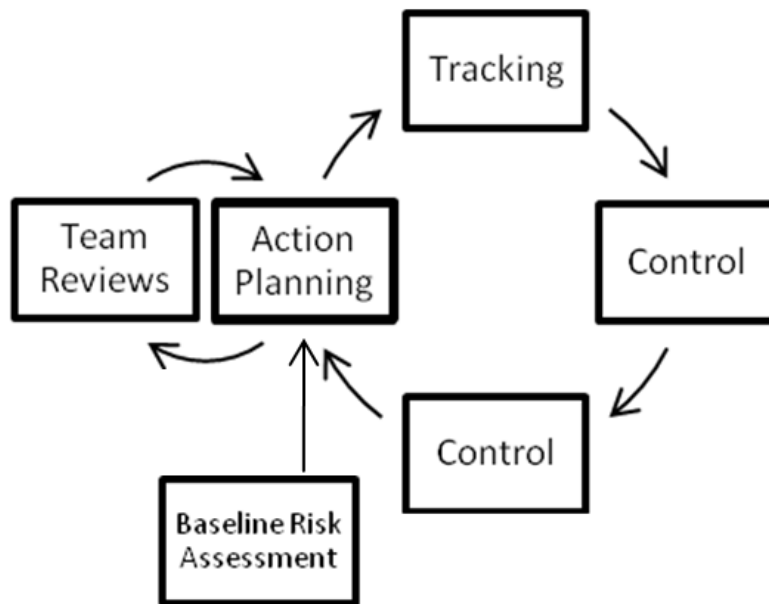


Figure 2: Team Risk Management Process Set

Team Risk Management[5] defines the organizational structure and operational activities for managing risks throughout all phases of the life-cycle of a software development program such that all individuals within the organizations, groups, departments, and agencies directly involved in the program are participating team members. Through the adoption of team risk management, the government and contractor are provided with processes, methods, and tools that enable both organizations, individually and jointly, to be increasingly anticipatory in decision-making processes". Team risk management practices bring all individuals from developers to customers within an organization. This technique ensures continuous risk management throughout the project iteratively and cooperatively. The processes of team risk management also address all five steps of the SEI paradigm through four processes. It combines the identification and analysis steps of SEI standards into the routine risk identification and analysis process. Risks not only exist in one stage but it can appear throughout the entire life cycle of a program. So this technique is a continuous process to identify and to control over risks. Here, a continuous cyclic set of scheduled activities are executed by team risk management for managing risks.

The working procedure of TRM are identify risks, regularly review and analyze new risks, plan for sensible application of resources to ease risks, tracking of risks and risk normalizing actions, start controlling of risks that turn into problems, and finally start communication about risks among all partners in the program.

C. Project Risk Management Framework

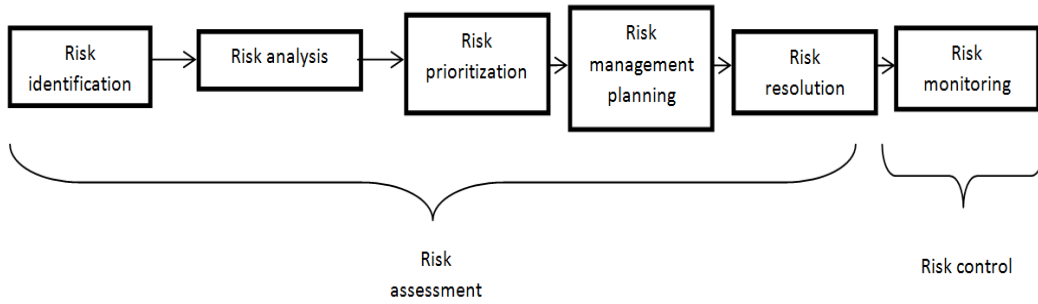


Figure 3: Project Risk Management Framework

Another model suggests that risk management includes two primary activities, risk assessment and risk control, each of which has three subsidiary steps [6], shown in Figure 3. Risk identification produces lists of project-specific risk items that are likely to compromise the success of a project. Risk analysis and risk prioritization rank the identified risk items by assessing the probability and severity of the loss for each risk item. Risk management planning defines how risk reduction will be conducted in a particular project by defining, among other things, risk-reduction tasks, responsibilities, activities, and budget. Risk-reduction activities must take into account the process, organization, and technology. Risk resolution produces a situation in which the risk items are eliminated or otherwise resolved. Risk monitoring involves tracking the progress of a project toward resolving its risk items and performing corrective activities where appropriate.

D. Project Risk Management Process

Figure 4[3] illustrates the risk management process. This process starts with the identification of a list of potential risks. Each of these risks is then analyzed and prioritized. A risk management plan is created that identifies containment actions that will reduce the probability of the risk occurring and/or reduce the impact if the risk turns into a problem. The plan also includes contingency actions that will be taken if the risk turns into a problem and the associated triggers (indicators that the risk is turning into a problem).

The containment part of the plan is then implemented and actions are taken. The tracking step involves monitoring the status of known risks as well as the results of risk reduction actions. If a trigger indicates the onset of a problem, the corresponding contingency plans are implemented. As new status and information are obtained, the risk management plans are updated accordingly. Tracking may also result in the addition of newly identified risks or in the closure of known risks.

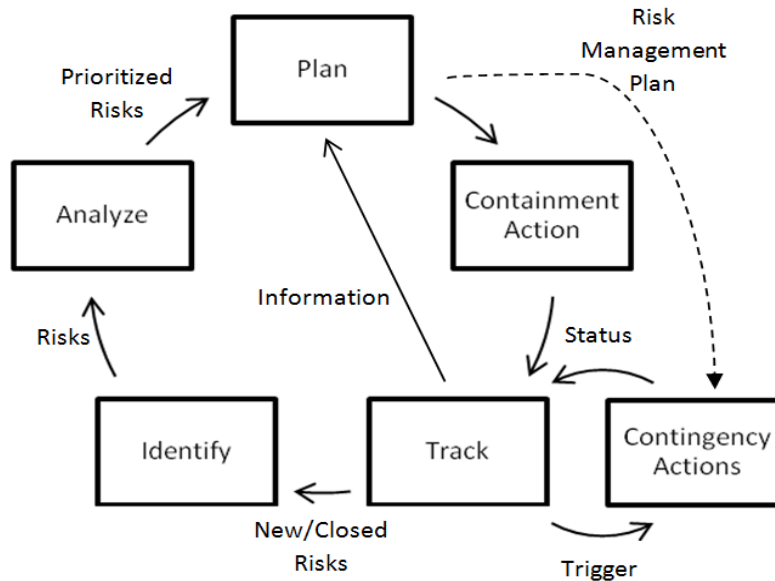


Figure 4: Project Risk Management Process

*E. Risk Management Processes*

Another approach suggests that risk management has following 6 steps: [2]

- Planning risk management: deciding how to approach and plan the risk management activities for the project
- Identifying risks: determining which risks are likely to affect a project and documenting the characteristics of each
- Performing qualitative risk analysis: prioritizing risks based on their probability and impact of occurrence
- Performing quantitative risk analysis: numerically estimating the effects of risks on project objectives
- Planning risk responses: taking steps to enhance opportunities and reduce threats to meeting project objectives

Monitoring and controlling risks: monitoring identified and residual risks, identifying new risks, carrying out risk response plans, and evaluating the effectiveness of risk strategies throughout the life of the project

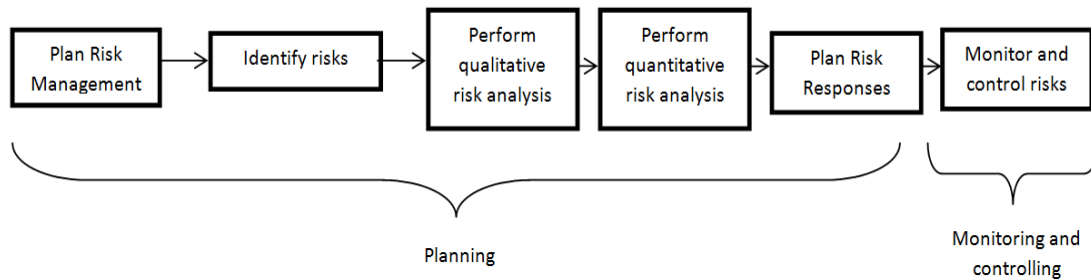


Figure 5: Risk Management Processes

*F. 'Soft Risk' Model*

As shown in Figure 6, risk management uses an eight-step process.[5][7] When any new risks are identified throughout the project, a five-step inner process is used to improve earlier estimates and judgments continuously. The first step in Softrisk model is Risk Identification.

Softrisk model identifies not only general kind of risk that can be occurred for any kind of project but also specific type of risk that only can be happened for some specific type of project. After risk identification in second stage of Softrisk model each identified risk is addressed in term of its probability and magnitude. Probability and magnitudes of the risks are estimated by a special checklist. Negligible, low, medium, high, very high and extra high are the categories under which risks are estimated. In risk documentation stage Softrisk documents all generic and specific risks data. This document is used for tracking projects situation, statistical operations and future risk predictions. Afterwards, risk assessment is done based on risk's probability and magnitudes. In fifth stage, RE valued are used to sort all risks and top ten risks for each inspection prioritized and listed. Then a graph is used to represent RE values by dividing three zones red, yellow and green. In controlling phase a suitable reduction technique is chosen based on severity of the risk. This technique could be mitigation, contingency or crisis plan. After using any of this reduction technique reassessment, re-estimation and re-documentation is required. And in the last stage of Softrisk model to be confirmed about non existence of any risk, this approach can be started from began.

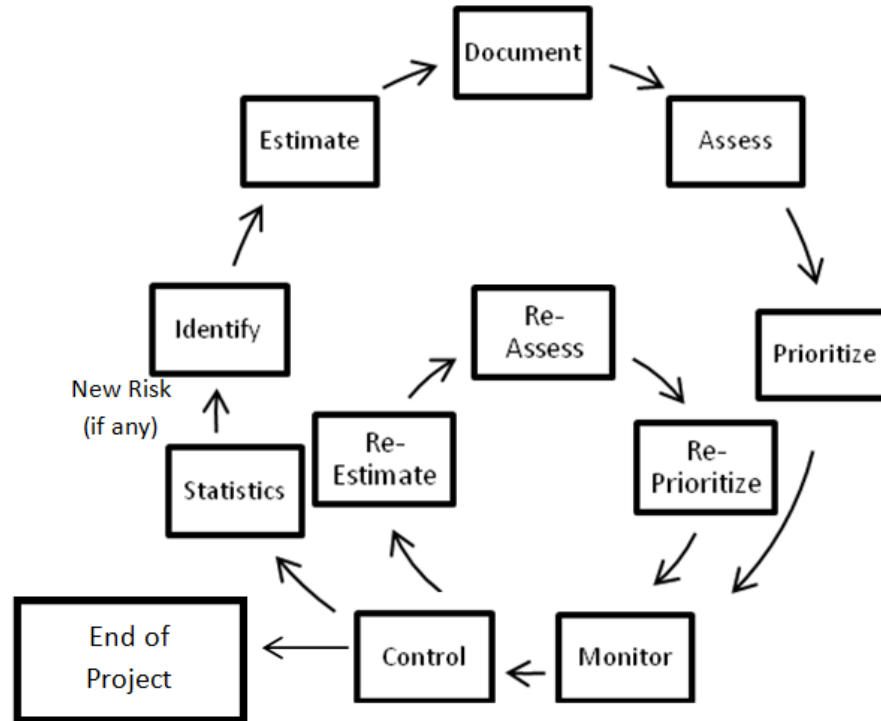


Figure 6: 'Soft Risk' Model

### G. Riskit Framework

Riskit [5] is a risk management method that has been developed to provide a theoretically sound as well as a practical risk management approach. The method used in a number of industrial projects in Europe and USA. The reason behind the developing of Riskit is to support systematic risk analysis. An effort has given to design the method preparing a goal of avoiding hazard section. Riskit approach supports qualitative analysis of risk situation. A graphical formalism is used by this tool. This technique can rank the risks, based on the availability of historical data, on accurate assessment and on utility theory. One feature of this tool is, it supports multiple goals and stakeholders. The Riskit analysis graph is a graphical formalism in Riskit model to document risk. Using the Riskit analysis graph different aspects of risk explicitly are defined. Hence it is more formal than face to face communication. The Riskit analysis graph decomposes risks into risk elements during the Riskit process. According to the figure 4 risk management infrastructures defines method, techniques, responsibilities and the scope of risk management in Riskit management cycle. It reviews the predefined goals for the project, refining them and also classifies implicit goals and constraints explicitly. Riskit model deals with all stakeholders of the project and with their associated goals.

According to the Riskit management cycle, it identifies risks and monitor in risk identification and monitoring phase. In risk analysis phase it pigeonholes identified risks into risk factor and risk events. Then it accomplishes risk scenarios for all risk events those have been classified in risk analysis phase and estimates risk effects for all risk scenarios. Afterwards, suitable levels of metrics are used to estimate probabilities and utility losses of risk scenarios. In risk control planning phase, a ranking of risk scenarios have made based on their probability and utility loss for each stakeholder. Controlling of risks in Riskit risk management, implements the risk controlling actions.

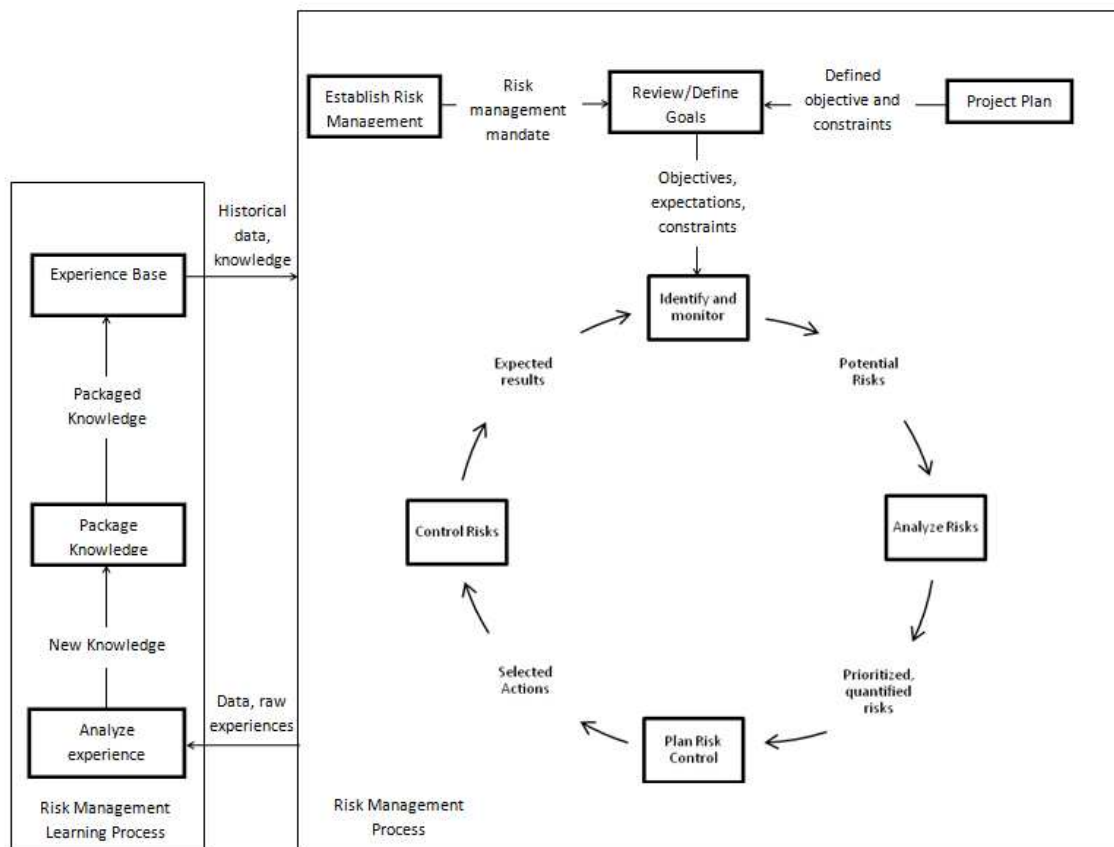


Figure 7: Riskit Framework

### III. CONCLUSIONS

This paper describes various Software Project Risk Management frameworks. These models or frameworks acts as tools to guide the project manager in order to perform efficient risk management. It is very important to identify critical risks involved in the project so that they will not affect the success of the project in future.

### REFERENCES

- [1] Li Guiling, Zhang Xiaojuan, "Research on the Risk Management of IT Project", E -Business and E -Government (ICEE), 2011 International Conference
- [2] Kathy Schwalbe, "IT Project Management"
- [3] Linda Westfall, "SOFTWARE RISK MANAGEMENT"
- [4] Abdullah Al Murad Chowdhury and Shamsul Arefeen, "Software Risk Management: Importance and Practices", IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 02, ISSUE 01, MANUSCRIPT CODE: 110740
- [5] Md. Forhad Rabbi, Khan Olid Bin Mannan, "A Review of Software Risk Management for Selection of best Tools and Techniques", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing
- [6] Jingyue Li, Reidar Conradi, Odd Petter N. Slyngstad, Marco Torchiano, Maurizio Morisio, Christian Bunse, "A State-of-the-Practice Survey of Risk Management in Development with Off-the-Shelf Software Components", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 34, NO. 2, MARCH/APRIL 2008
- [7] Y.H. Kwak, J. Stoddard, "Project risk management: lessons learned from software development environment"