A Preventive Risk Analysis for Managing Distributed Software Projects based on Deliverable

Yumnam Subadani
Manipur Institute of Management Studies
Manipur University
Canchipur, Manipur, India

L. Prabhakar
Manipur Institute of Management Studies
Manipur University
Canchipur, Manipur, India

ABSTRACT
In a distributed software development environment, software projects are geographically distributed with minimal face-to-face interaction between team members. Recent software functions are delegated to popular open source software projects: -examples like Mozilla Firefox, Google Chromium, Android and the Apache OpenOffice Suite, etc. So the managers must know how to perform distributed projects and its team. Most of software risk management is done throughout the whole project from inception to commissioning. The aim of this study is to understand the need for the risk assessment and management based on deliverable for both agile and traditional methods of software development process. In this study, the authors propose a model, where the protective risk analysis can be done based on the deliverables, so that require mitigations can be provided. Mitigation factors can be also based on the seriousness of the deliverable

Keywords
Distributed environments, risk factors, deliverables

1. INTRODUCTION
Deliverable is a term used in project management to discuss a tangible or may be intangible object that produced as results of the execution of such project that are intended to be delivered to clients or individual. Such deliverable could be inform of a report, a document, a server upgrade or any other related outcomes of an overall project. It may be composed of several smaller deliverables or associated deliverables. It may be either a conclusion to be achieved or an output to be provided.

Software managers need to know the ways to build up a project teams across sites, to distribute tasks, to share information across time, space, and to coordinate effort to build coherent outcomes [1]. Economic forces are relentlessly turning national markets into international share and spawning forms of highly competition and closely cooperation that reach across global boundaries. Attention has turned toward trying to understand the factors that allow global multinationals and virtual groups to operate successfully across globe geographic and across the cultural boundaries. There are lots of risks and problems in risk resolution techniques also handling the framework for managing risks in distributed contexts. We all agree that *we can neither predict nor control what we cannot determine.* Consistent measurement is a key element in establishing a scientific basis for software engineering [2]. At the heart of Information systems the risk and safety aspects play a vital role. Risk management is essential in achieving a successful project outcome.

The following is some of the problems facing in such environment.

1. Requirement gathering

It is to collect the exact requirements from customers and research among the entire teams and to facilitate successful communication for the entire project. This phase is the trigger point of all types of risk [3].

2. Communication

During the software lifecycle, team members change a large amount of data using different tools and different formats. It encounters misunderstandings, excellent response times and security problems. Such the degree of distribution of the work and team grows, coordination and synchronization become more complex, and traceability becomes a critical factor.

3. Knowledge Management

Sharing the experiences, methods, decisions, and skills that accumulated during the software lifecycle is not easy task in distributed environment. Knowledge creation and acquisition of knowledge are becoming more difficult task in distributed software development projects. Selection of appropriate tools for knowledge management is extremely critical.

4. Quality Management

Reviewing of something requires often interaction and feedback. Quality of the work must not only be limited and considered to software products but also to development processes, which significantly influence product quality.

5. Risk Management

Communication problem among the team members leads to other problems like coordination, problem resolution, group awareness, information sharing following a traditional practices and risk identification [4]. Rules and guidelines with which to conduct the teams and their interactions become necessary. Teams must be continuously controlled in order to solve problems, take corrective actions, and the use of appropriate measures is a vital key factor [5].

2. LITERATURE REVIEW
The reason for distributing software development can continue to increase time-to-market by around the-clock to increase flexibility on merger and acquisition different opportunities. Such activity of geographical distribution becomes increasingly with a high transfer of development and maintenance activities from the developed countries to developing countries [6]. Other reasons include access to cheaper labor, increasing demands of customers and

conditions by local market proximity, or could be by capitalizing on the global pools of knowledge [7]. In fact, lack of high skilled science and engineering expertise and, more generally, needs for access to trained personnel are significant explanatory factors for off-shoring innovation decisions [8,9]. In such way, the distributed software development it is a business necessity to meet the demand of the current scenario [10]. Besides this knowledge sharing across the country for the software development projects are becoming a trend in the software industry. In such a distributed environment the coordination and communication proving difficult, project management becomes even more challenging. Distributed software development has its unique complexities, and challenges. Such characteristics range from technical, economic, organizational, and cultural issues. This arises from different time zones, languages, and geographical locations. Making distributed project teams' work effectively, and delivering quality outcomes on time and within budget, is therefore a significant industry-wide challenge for this era. In response to these challenges, experts, researchers and practitioners are continuously finding and developing vast amounts of frameworks, guidelines, tools, methodologies and tips [11].

Fig1: Typical Distributed Software Projects environment

2.1 Information System Security Risk Management (ISSRM)

Practitioners have developed ISSRM methods to help determine the relative importance of security project risks and the cost-effectiveness of solutions to address them. The methods are primarily driven by standards and professional best practices in the domain of security and risk management. The protective security enables to mitigate the risk probability.

2.2 General common framework for risk management

The initial phase of framework aims to prepare the risk management project by providing the managers with the cost of the project and the schedule of the different security activities. It gathers information about the analyzed system. Weaknesses and security breaches of the analyzed system are identified at this level. It identifies the attacks that threaten the analyzed system. It identifies the risks that may threaten the assets of analyzed system based on the identified vulnerabilities and threats proposing a security strategy mitigating the identified risks. It defines the security policy that will be adapted by the analyzed system to mitigate security risks and selected security countermeasures are implemented according to the security policy. It maintains the analyzed system in an reasonable security level. Monitoring activity can result in the re-execution of some processes if needed. It also reacts to security intrusions according to the incident response plan.

2.3 Security attributes

Every security project has four constraints or forces to provide a success to it. They are scope, time, cost, and quality [12].

1. Scope:

The scope or the work structure is the total amount of work to be accomplished during a project cycle. A tight budget may enforce the reduction of security areas that will be the cause of the security project plan. The choice of the scope has to be done carefully to ensure that the corporate demands locally and globally.

2. Time (Schedule):

Every project requires a certain amount of time to complete. A schedule is developed after the definition of the work to be accomplished, and the necessary resources are compiled. If the schedule has to be shortened, the project's scope and quality might have to be reduced.

3. Cost:

Budget spent on security must be justified in economic terms. Security expenditures must then be balanced with these losses in order to avoid such waste in the coming years.

4. Quality:

The quality of IT security project plan often comes down to the amount of testing and analysis that is done prior to, during, and after project implementation.

2.4 General Risk management

During the risk management, an organization prevents or reduces the risk. The impact of the management of the team knowledge has on the project cost. A team with low skills and experience faces problems in analyzing security breaches and risks and in proposing the correct decisions that mitigate the risks. Three kinds of problems are reported in this case.

1. The first one is related to the delays caused by the slowness of the team in performing their activities.
2. The second problem is related to the risks that are not identified and therefore not mitigated or to the non effectiveness of security solutions.

3. The third problem is specific to incident response team members and is related to the delay in responding to security incidents.

The mentioned problems cause losses to the organization running the security project [13]. Most of The available frameworks do research of the risk of the project based on phases or schedule of the projects. Studies of relating a risk and its exposure based on the deliverable are not been caries out. Only things never change during a project and its phase is the deliverables. The customer and projects team are required to understand the amount of risk and its exposure associated with any kind of deliverable.

3. PROPOSED FRAMEWORK FOR MANAGING DISTRIBUTED SOFT-WARE DEVELOPMENT PROJECTS

It will be a preventive risk analysis for Managing Distributed Software Projects based on the identified deliverable of the projects. Team and resources could work and update from any part of the globe. The main goal that they will maintain and share is the input and process to produce the deliverable. Each deliverable will have its own prerequisite for all those involved.

The goal of this study to minimizing the risk at the lowest level while managing such a distributed software projects. The study will consist of the following process:

1. Listed out the possible deliverable of a project
2. Identify the associated factors like input, process and required resources of a deliverable.
3. Analyze the risk of associated factors of a deliverable
4. Evaluate the risk of associated factors of a deliverable
5. Evaluate the TOTAL risk for a deliverable
6. Risk decision satisfactory? If yes, go to step 7, otherwise go to step 2
7. Provide the possible preventive measures of the risks

All the process will be supported by a monitoring system and communication system to links all the teams and resources under a single project environment. Pictorial representation of the proposed framework is shown in figure 2.

Advantage of this framework is that it is based on deliverable and its associates risk analysis. It does not require any risk analysis expert to determine the risk. The framework can be used in the identification and assessment of risk in any organization without giving any extra effort and time. The risk identification activity can be merged with the task identification activity based on any deliverable.

Each deliverable will comprise of one or more associated factors. Each of factors can then be processed to calculate the risk exposure. This can be estimated by making a list of the deliverable and its associate factors which could generate a risk. The measure unit of the impact of the risk for the associated factor can be categorized as negligible, marginal, critical or catastrophic. Once the impact is ascertained for each factor that could generate a risk, risk exposure of a factor can be calculated as equation (1).

$$RE_{AR} = \sum_{i=1}^{e} (F_i * I_j) \quad \text{.....(1)}$$

Where, $RE_{AR:}$ Risk Exposure for associated factors of a deliverable (AR-Associated Risk)

F: Frequency of checking of each factor i,

I: Impact on an entity for each factor i

e: Total numbers of factors that lead to the failure of deliverable.

Total risk exposure of a deliverable can be calculated as given in equation (2)

$$RE_D = \sum_{AR=1}^{T} RE_{AR} \quad \text{.....(2)}$$

Where RE_D is the overall risk exposure for a deliverable (D).

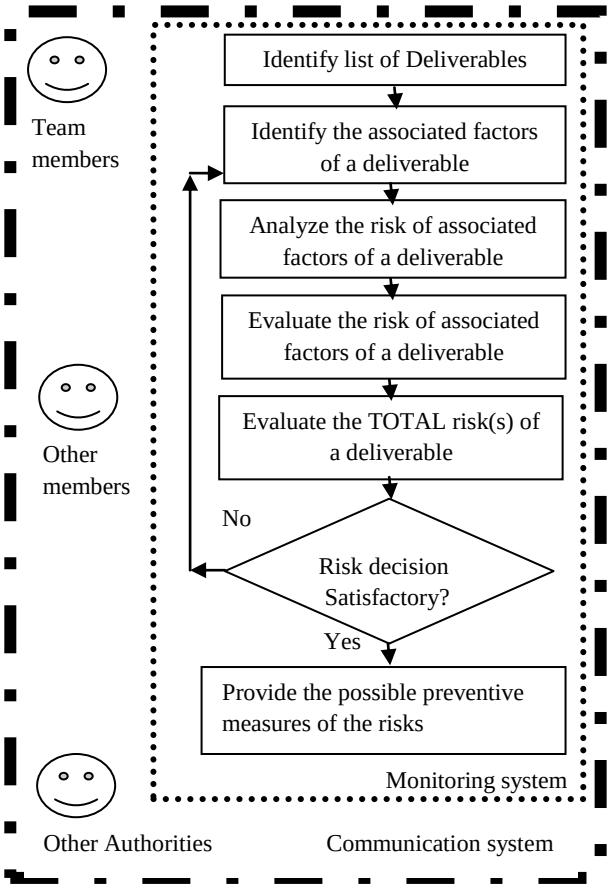

Fig2. The proposed framework of risk analysis

It is possible to get the response to frequency of occurrence can be categorised as frequent, likely, most likely etc. and impact may be described as catastrophic, critical, marginal etc. To incorporate these responses fuzzy logic is a suitable alternative for risk assessment.

4. A CASE STUDY AND ITS RESULTS AS PER THE PROPOSED FRAMEWORK

Our goal is to calculate the overall risk exposure of a deliverable after calculating each associated risk factors of a

single deliverable and so on for a list of all deliverable of a project. Let's consider basic deliverables taken from our open source projects.

Deliverable1:
"Design the layout of a Monthly Report format"
This task requires verifying that report Design Layout has been done as per the requirement of the customer.

Deliverable2:
"Verify the Printed Monthly Report for a month"
This task requires verifying and validating the Printed Report as per the data provided from the customer for a month.

Considering the Deliverable1 of verifying that report Design Layout, there are two possible factors which may cause the deliverable to a failure.

(a) Is the layout design as per specified by the customer?

(b) Is the designed layout verified by a customer?

An evaluation criterion is considered by introducing the frequency of occurrence of failure in terms of most likely, likely and unlikely. This is only a measure for execution and may include other intermediate steps for more accurate assessment of the frequency. For the given example, we have considered the following:

(a) Is the layout design as per specified by a customer?
: Likely

(b) Is the designed layout verified by a customer?
: Unlikely

4.1 Frequency of occurrence

The Frequency of occurrence is to be given some numerical value so as to enable the assessment of Risk Exposure and for the purpose of illustration using graphical aids. We have considered - 'unlikely' to be 1, likely to be 2 and most likely to be 3.

4.2 Risk Impact factor

The Impact of a risk could be catastrophic or critical or average or marginal or no impact. This can be quantified by assigning 5 for catastrophic, 4 for critical, 3 for average, 2 for likely and 1 for unlikely situation. This can be defined by the organisation as this framework is intended for any type of organisation and nothing can be made rigid in this case. This also depends on the risk acceptance capacity of the organisation, project, scheme etc. The Risk Exposure in case of the two associated factors can be represented in table1.

Table1. Associated factors for Deliverable1

Associated factors for Deliverable1	Frequency	Impacts
1. Is the layout design as per specified by a customer?	Likely (2)	Critical(4)
2. Is the designed layout verified by a customer?	Unlikely (1)	Average(3)

The risk exposure RE of factor1 and 2 can be calculated as

$RE_{A1}=2*4=8$ and $RE_{A2}=1*3=3$

Therefore, the total RE for the deliverable1 (factor 1 and 2) is:
$RE_{D1}=8+3=11$.

Now we consider the Deliverable2 i.e. Verify the Printed Monthly Report for a month. Considering the same criteria as in the previous deliverable, the RE for deliverable2 is identified.

Table2. Associate Factors for deliverable2

Associate Factors for deliverable2	Frequency	Impacts
1.Verifying & validating the Printed Monthly Report	Likely(2)	Catastrophic(5)
2. Verify & Validate the Printed Monthly Report for "March 2013"	Likely(2)	Critical(4)

In terms of figures we can express as follows:

$RE_{A1}=2*5=10$ and $RE_{A2}=2*4=8$.

Therefore, RE_{D2} for the task no. 2 is: $RE_{D2}=10+8=18$.

4.3 Comparison of risk exposures of two deliverables

In both cases, we have considered associated factors those may cause failure of the deliverable. A limit of 2 factors is considered for execution, which may be increased depending on the modes of failure of the tasks of the organisation. The outcomes of the study can be a representation as figure3.

This representation indicates the risk exposure of the two deliverables which can form a ready reference to identify those tasks which needs more analysis to initiate or intensify the risk control measures. The factor(s) of a deliverable which involve larger areas need more attention. Therefore, it is understood that Risk Assessment must form an integral part of every organisation, project, scheme etc. So as, to identify those associated factors of deliverable(s) that require further risk monitoring and control measures to minimise loss of any form.

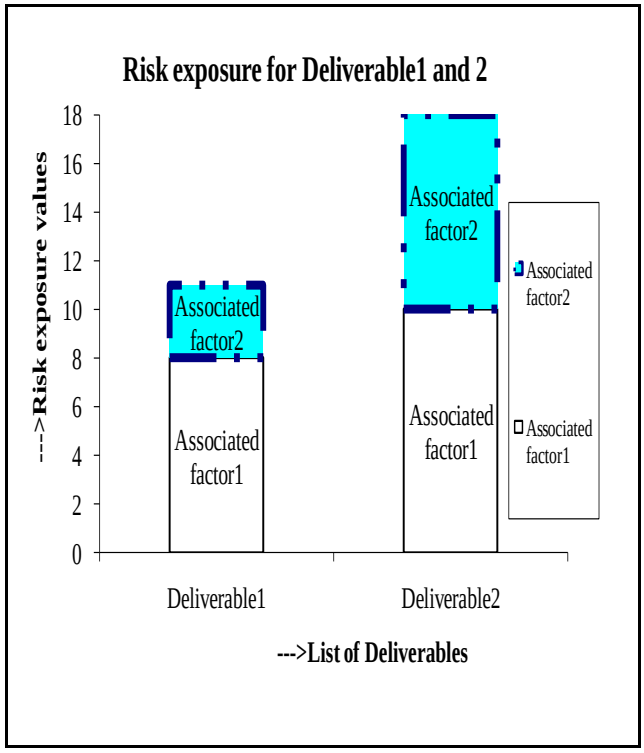

Fig3. Comparison of risk exposures of associated factors of two deliverables

5. CONCLUSION

Most of the earlier studies consider the many major components of a project to analyze the risk of a project taking the serious guidance from the experts [14,15].The aim of the risk analysis process is to determine the main risks relative to each deliverable leading to every main risk. The proposed framework considers risk identification and assessment based on the deliverable only. It also considers the associated factors which may lead to a failure. The framework is simple to implement and will help to identify the events that are more vulnerable and needs more attention. This in turn will minimize the consequences that could have happened if this analysis was not done to determine the critical points which are exposed to risk. If the team members are sure about the deliverables, finding the risk associated could be easy by using such a framework.

6. REFERENCES

[1] J.D. Herbsleb and D. Moitra, "Global Software Development," IEEE Software, vol. 18(2), 2001, p16–20.

[2] T. DeMarco. Controlling Software Projects. Yourdon Press, New York, 1982.

[3] Darja Smite, Requirements Management in Distributed Projects, Journal of Universal Knowledge Management, vol. 1, no. 2 (2006), 69-76

[4] R. Sangwan, M. Bass, N. Mullick, D. J. Paulish, and J. Kazmeier,Global Software Development Handbook (Auerbach Series on Applied Software Engineering Series), Auerbach Publications: Boston, USA, 2006.

[5] Miguel Jiménez1, Aurora Vizcaíno and Mario Piattini, "Improving Distributed Software Development in Small and Medium Enterprises", The Open Software Engineering Journal, 2010, 4, 26-37

[6] Meyer, B. "The unspoken revolution in software engineering," IEEE Computer (39:1), 2006, p121-123.

[7] Conchuir, E.Q., Olsson, H.H., Agerfalk, P.J., and Fitzgerald, B. "Benefits of global software development: exploring the unexplored," Software Process: Improvement and Practice, 2009.

[8] Lewin, A.Y., Massini, S., and Peeters, C. "Why are companies offshoring innovation? The emerging global race for talent," Journal of International Business Studies, 2008.

[9] Manning, S., Massini, S., and Lewin, A.Y. "A dynamic perspective on next-generation offshoring: the global sourcing of science and engineering talent," Academy of Management Perspectives, 2008, pp 35-54.

[10] Damian, D., Sengupta, B., and Lanubile, F. "Global software development: where are we headed?," Software Process: Improvement & Practice(13:6), 2008, p473-475.

[11] Espinosa, J.A., DeLone, W., and Lee, G. "Global boundaries, task processes and IS project success: a field study," Information Technology & People (19:4), 2006, pp 345-370.

[12] S. Snedaker, IT Security Project Management Handbook,Syngress, 2006.

[13] Jihene Krichene, Managing Security Projects in Telecommunication Networks, Ph.D. THESIS, Nov 22, 2008

[14] T. N. Nguyen, "A decision model for managing software development projects", Information & Management,2005, 13-25

[15] Nakatsu, R. T., C. L. Iacovou. 2009. A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. Information & Management 46(1) 57–68