International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 6, Issue 1 (Jan-Feb 2018), PP. 32-39

NOVEL RISK MANAGEMENT IMPLEMENTATION APPROACH

Suruchi Shukla[1], Dr Anshu Srivastava[2],
[1]Research Scholar, Shri Venkateshwara University, Gajraula,
[2]Research Supervisor, Shri Venkateshwara University, Gajraula,
UP, India

***Abstract*— All risk management steps (e.g. identification, estimation, evaluation, planning and controlling) are included in the modules of this segment. However, the techniques used and the manner of conducting these steps could be different from other approaches, as they are designed to accommodate the distributed development nature and needs. For instance, aspects such as sites dependencies, which are related to distributed development, are considered. Atypical risks are also treated in this segment.**

***Index Terms*— Novel risk, RE, DDF, TREV, evaluation module, Magnitude.**

I. RISK MANAGEMENT IMPLEMENTATION SEGMENT

The Risk Management implementation segment ensures continuous risk management implementation for the 3P perspectives of the distributed development. As Table 1 shows, the Risk Management implementation segment consists of six modules (Clustering Module, Risks Repository Module, Estimation Module, Evaluation Module, Atypical Risks Module and Planning and controlling Module). These modules are described in detail in the following subsections.

Table 1: Risk Management Implementation Segment

Module	Description	Inputs	Outputs
Clustering Module	Any potential risks to distributed environment should be clustered from the 3P perspectives before being	Risk data , clustering criteria	Clustered risks from 3P perspectives
Risks Repository Module	Cards are issued for all risks and saved in this repository. Each card has a unique number and contains all main data about the risk. To help developers/managers to identify the risks, the risks repository is initiated with cards for all known distributed environment potential risks.	Current cycle identified risks and any potential risks	Risk cards clustered from 3P perspectives and made available for use during the risk management cycles
Estimation Module	This module estimates the risks with consideration to distributed development factors. It uses two estimation equations RE and TREV and DDF estimation matrix	Risks cards and related information that could be used to estimate risks probabilities , magnitudes distributed	RE, DDF, TREV values
Evaluation Module	To evaluate the risks	Estimated identified risks (RE/TREV values) and atypical risks, project and risk card	Top risks (most critical) and prioritized risks based on RE/TREV values

Atypical Risks Module	To deal with and absorb new unpredictable risks (atypical risks)	Atypical risk	Absorbing actions, and risk card
Planning and Controlling Module	This module deals with the preparation of plans and pre-cautions to deal with the risks	Ideas, experience, historical experiment, learned lessons, risks cards	Update risks card with plans (Who, What to , needs ,..)

II. RISK MANAGEMENT CLUSTERING MODULE

Proposed approach includes several concepts, which could help in tackling some of the identified weaknesses in the existing software risk management approaches. One of these concepts is the consideration of the risks from the 3P perspectives. This concept depends on a clustering strategy which uses special criteria to deal with the risk from these three perspectives. The clustering strategy is intended to save time and effort. It locates fewer resources for each perspective, as the management of risks will focus on the relevant perspective risks each time. Proposed approach suggests some factors that could help to cluster the risks from the 3P perspectives.

III. RISKS REPOSITORY MODULE

The Risks Repository Module has a vital role in the risk management process as it is the core of the risk identification process. It provides a preliminary list of distributed development potential risks. The risks are clustered from the 3P perspectives and made available for use during any Risk Management cycle. Any risk has a unique card, called a "Risk Card" (see Table 2), which contains the main risk data (e.g. risk reference number, name, perspective, potential impact and suggested control plan). A risk card needs to be built for any new identified risk before adding it to the risks repository. The risk repository can be used by all stakeholders, sites, developers and managers and could also be used for statistics and learned lessons. Generally, the data in the risk card are almost fixed data (descriptive data), but they might be updated if there are any changes related to the risk (e.g. controlling strategies). Table 2 is an example of a risk card. As can be seen in the table, the risk card contains all essential description data

Table 2: Risk Card Example

Risk ID	R11
Risk Name	Not enough experience with web services
Risk Source	Programmer 3
Aspect	Technical Risks
Perspective	Process
Risk Description	The programmer should have enough experience with Java and web services, but he has only experience with Java applications.
Risk Factors	The time is too short to learn web services; Not enough time to hire programmers; Not enough experience.
Potential Impact	Extra Cost (e.g. it costs 300 per a day for any delays)
Potential Affected Areas	Web related aspects
Dependency	All linked sites could be affected
Risk Management plan	Plan Ref. No.: P-Cu-011 Summary: Fast training course, postponed web ser- vice part, changing the type of the application or hire programmer
Primary Precautions Plan	Provide necessary training early Hire extra programmers if the time is short, but if there is enough time and less dependency train the existing programmers.
Card Issue Date	18/11/2017
Risks combination consequence	There is no other risk which has a combination effect with this risk

IV. RISK EXPOSURE (RE) EQUATION

RE is a famous equation and has been used for many years to estimate software risks. It depends on the estimation of the probability and magnitude values of the risk. There are different ways (qualitative and quantitative methods) to estimate the probability and magnitude. Although quantitative estimation is much more precise than qualitative estimation, people usually prefer to use qualitative estimation, because they find it much easier.

The RE equation has been used for the assessment of collocated software development since the late 1980s. However, the software industry is an evolving and rapidly growing industry, especially with the new phenomenon of distributed software development. Therefore, a new set of factors are involved which could have an effect on the risks and need to be considered in the estimation equations. For distributed development risk estimation, the RE equation could be improved by including the distributed factors. The TREV is an attempt to produce an improved equation for this purpose with consideration of the distributed factors.

To make the probability and magnitude estimation easy and to avoid any subjective and confusing issues, Table 3 is designed to help the users to estimate the probabilities and magnitudes of risks and can be used alongside the estimation line. The table is adapted from the Qualitative Risk Analysis.

Table 3 Probability and Magnitude Estimation Guide

Risk Probability Estimation Guide	
Negligible	Seldom occurs
Low	Unlikely to occur
Medium	Could occur
High	Will probably occur
Extremely High	Will almost certainly
Risk Magnitude Estimation Guide	
Insignificant	Lowest impact on goals and functions
Minor	Would threaten an element of the function
Moderate	Necessitating significant adjustment to overall function
Major	Would threaten functional goals / objectives
Severe	Highest impact on goals and functions

Table 4 establishes an example of using the estimation line to estimate risk probability, risk magnitude and risk exposure.

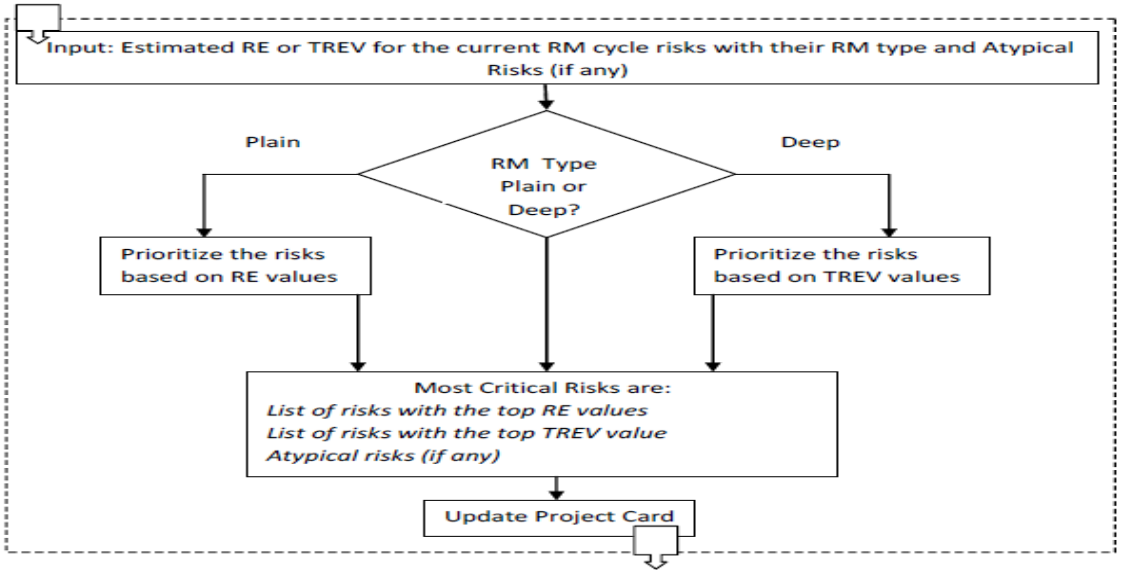
Table 4 Prob. and Mag. Estimation Line and Risk Exposure Example

Risk ID	Probability of the risk	Prob. Value	Magnitude of the risk	Mag. Value	Risk Expo-sure
R32	There is a high chance of the risk occurring but not certain	High = 0.75	Not worth mention-ing impact on any of the project aspects	Insignificant = 1	RE=Pro.*Mag RE= 0.75 * 1 = 0.75

V. EVALUATION MODULE

The evaluation module aims to evaluate the estimated risks in order to control them. The evaluation could be based on RE or TREV values. Since there are two types of Risk Management (Simple and Profound), the estimated risks could be mixed (RE and TREV) in the same Risk Management cycle. Therefore, the evaluation module evaluates the risks separately based on the type of Risk Management and estimate equation used. The separation is due to the following considerations:

Figure 1: Evaluation Module



The typical risks are always included with the most critical risks and they should be treated as top risks, because usually there is not enough time or information to estimate their RE or TREV and thus they might have higher priorities than others. The remaining identified risks can be accessed through the project card when it is needed, and updated with the evaluation module output. Focusing on the management of the top risks first is intended to save developers/managers time and effort, especially when the resources are limited.

Table 5: Example of All Estimated Risks

Risk Manage	Risk ID	Estimation Equation	Estimated Value
W1-C1	R7	RE	2.25
	R32	RE	0.5
	R18	TREV	6.25
	R5	RE	l
	R21	TREV	16.5
	R9	TREV	20.25
	R2	RE	1.5
There are no atypical risks			

Table 6: Example of Prioritized Estimated Risks

	Prioritized based on RE		Prioritized based on TREV	
Risk Manage	Risk ID	RE	Risk ID	TREV
W1-C1	R7	2.25	R9	20.25
	R2	1.5	R21	16.5
	R5	1	R18	6.25
	R32	0.5		
There are no atypical risks				

The examples in Tables 5 and 6 demonstrate how a number of identified risks are evaluated in this module. The first table (Table 5) shows all the estimated risks before the evaluation. In this table, all estimated risks are listed randomly without any sorting (mixed from RE and TREV). In the second table (Table 6), the risks are prioritized and grouped based on the evaluation equation (RE and TREV).

VI. PLANNING AND CONTROLLING MODULE

Any identified and evaluated risks need to be managed before they become a threat to the development progress (e.g. schedule overrun, low quality or extra cost). The propose approach provides a planning and control module to manage the identified risks. To maintain the flexibility of the proposed As can be seen in Figure 2, the planning section involves two types of plans: pre- cautions and reduction. Precaution plans are simple and could be valid for more than one risk when there are similarities between them. They involve some precautionary measures that are usually taken before the risk has occurred. These precautions are intended to avoid the occurrence of risks before they attack the development perspectives. These precautions should be simple, not costly and be carried out at any time. It is advisable that they are designed early and become available for use quickly. The history of similar risks and development is helpful for the preparation of precautions.

The second type of risk management plan is the reduction plan, which is intended to be used when the risk has already occurred. The reduction plans are designed carefully to control the risks and reduce their impact. These reduction plans consist of a number of steps that are performed systematically when a risk has occurred and tells the user what to do, how to do it, and which resources are required. Experience, brain storming, historical data and learned lessons help to design these plans.

modules, the planning or control sections can be activated individually based on need (see Figure 3.10). For instance, the planning section can be activated early simultaneously with the building of risk cards to include the plans as a part of the risk cards.

The control section (see Figure 2) in the planning and control module is responsible for the implementation of the risk management plans. The precaution plans are implemented before the risks have occurred, but the reduction plans are performed when the risks have already occurred. The control strategy in the proposed approach focuses on the most critical risks first (at the top of the RE, TREV and atypical risk list). The selection of the most critical first is because of their expected higher impact on the project compared with others. This does not mean ignoring the other risks. In fact, all the identified risks must be controlled, but because of the resource avail- ability and limitations, the most critical risk should be controlled first. At the end of any controlling operation, the risks need to be re-assessed and then re-evaluated, and the project card should be updated with the newer results and learned lessons could be extracted as well. Controlling the risks does not mean the end of the risk management process. Risk Management is a continuous operation and new risk management cycles will be conducted until the risk management project is closed

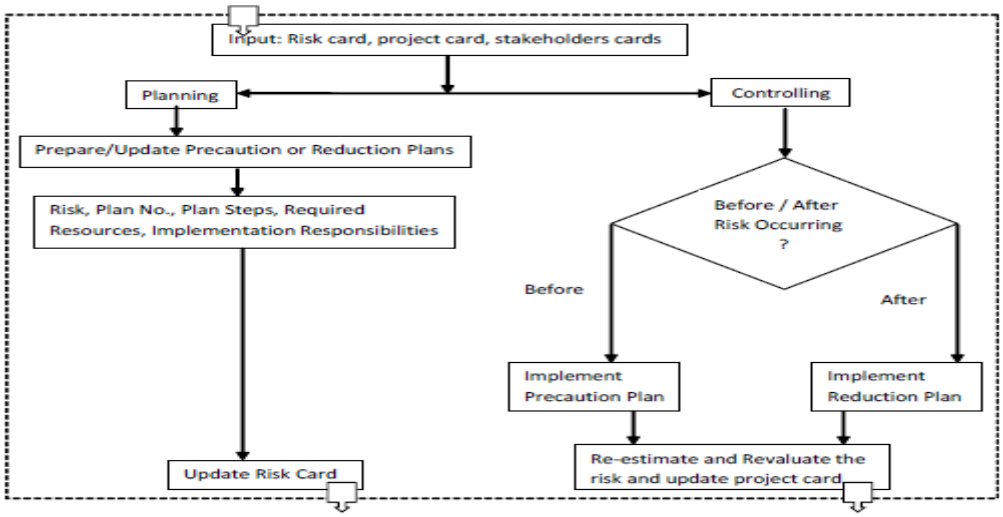


Figure 2: Planning and Controlling Module

VII. EVALUATION AND EVOLUTION SEGMENT

As Table 7 demonstrates, the Risk Management Evaluation Auditing segment consists of two modules: the Risk Management Evaluation and Auditing Module and Risk Management Evolving Regulator Module. The aim of Risk Management Evaluation and Auditing Module is to monitor the performance of the Risk Management process and to monitor the risks of any desired risk management cycle. Monitoring the risks gives information about the risk threat levels during the Risk Management cycle. This ensures that all the risks are always monitored before and after controlling them. Monitoring of Risk Management processes performance gives information about the efficiency of the Risk Management process in general. The Risk Management Evolving Regulator Module is responsible for making any required improvements or modifications to the proposed approach.

Table 7: Evaluation and Evolution Segment

Module	Description	Inputs	Outputs
Risk Management Evaluation and Auditing Module	A module to evaluate the progress of the risk management process which is used for monitoring purposes and taking necessary correctiv	Project card, any gathered comments or suggestions	Performance re-port
Risk Management Evolving Regulator Module	Evolving module is responsible for making any required improvements or modifications to the proposed approach	Performance report	Evolution Plan

VIII. Evaluation and Auditing Module

The Evaluation and Auditing module gathers data during the Risk Management cycle via the input component (see Figure 3). The input data include project card, auditing evaluation and developers'/managers' comments and suggestions.

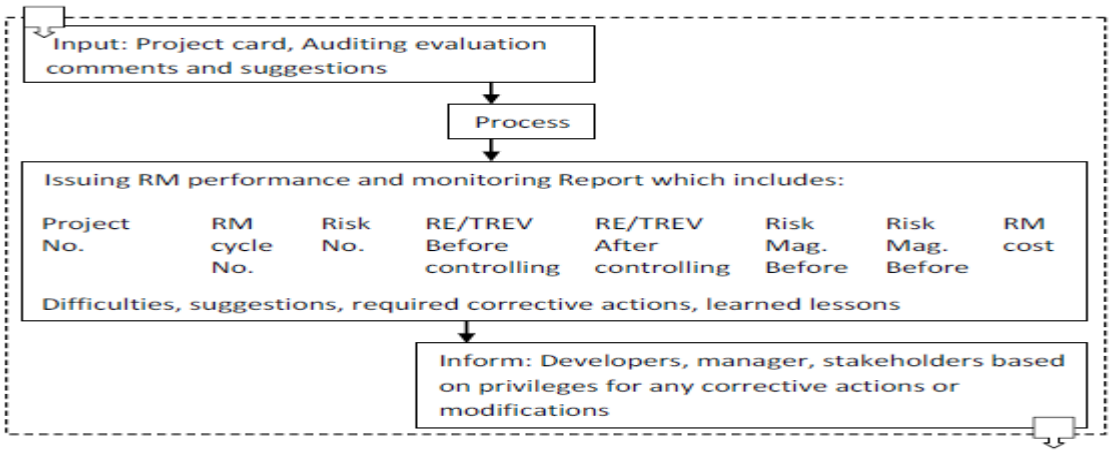


Figure 3 Evaluation and Auditing Module

The comments and suggestions reflect problems and difficulties that are faced during the Risk Management process and any improvement ideas to enhance the approach or Risk Management process. After inputting the related data, the next step is the processing of the collected data, which leads to producing a Risk Management Performance and Monitoring Report. This report, as shown in Figure 3 contains important information about the Risk Management performance, risk situations before and after being controlled, and any suggestions or comments. All of this information is linked with the project, Risk Management cycle and risk numbers. In fact, the report is intended to monitor Risk Management efficiency and also helps to effect any necessary change (corrective actions) to the proposed approach. Finally, the developers, managers and stakeholders involved in the desired Risk Management cycle receive a report based on their privileges, so that they can decide to take any corrective actions or even suggest some modifications and evolvement to improve the proposed approach, to improve the Risk Management process or tackle any weaknesses. Any suggestions in this regard are passed to the Risk Management evolving segment.

IX. Risk Management Evolving Regulator Module

The proposed approach is designed to be ready for any necessary future modification or improvement. It has a special module to handle such modifications, called the Risk Management Evolving Regulator module. As established, the evolving module is in- tended to receive improvement and modification needs and suggestions and make the decision to evolve the Risk Management process and proposed approach. The Risk Management Evolving Regulator Module (see Figure 4) is responsible for regulating all evolving operations on the proposed approach.

As input, the module collects all evolution needs and suggestions in a repository called the "Evolution Box". All of the evolution box contents, including the performance report, are discussed by an evolution approval board. Periodically, this board has scheduled meetings to analyze the contents of the evolution box and decide what sort of evolutions need to be made to the Risk Management process. The evolutions occur as new or modified steps, components and techniques. The board issues an evolution plan which indicates the implementation priori- ties, required cost, required resources, affected layer/components, necessary training, responsibilities and implementation schedule. The next step in this module is

the implementation and evaluation of the evolution plan, which is carried out by the manager/developer who uses the proposed approach.

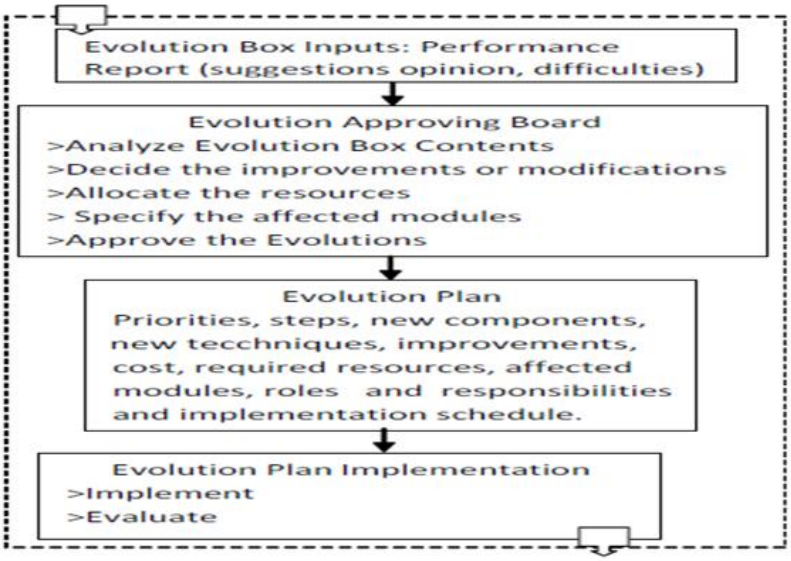


Figure 4: Evolution Module

X. CONCLUSION

Therefore, the proposed approach supports Risk Management communication via a special channel called the communication channel (see Figure 3.1). The purpose of the channel is to ensure internal and external Risk Management communication and data exchanges during the Risk Management cycle. The communication could be internal communication between the phases or modules, or it could be external communication with the other related approaches or sites. For this purpose, all electronic media can be used. Furthermore, all exchanged data must be documented and controlled based on privileges and permissions. The communication channel provides this support continuously during all Risk Management stages with consideration to security restriction issues.

REFERENCES

[1] APM (2011) APM Body of Knowledge 5th Edition, APM Definitions, online at www.apm.org.uk/sites/default/files/Bok%20Definitions.pdf

[2] Olsson, R. (2008) "Risk management in a multi-project environment: An approach to manage portfolio risks", International Journal of Quality & Reliability Management, Vol. 25 No. 1, 2008 pp. 60-71

[3] Elky, S (2006) "An Introduction to Information System Risk Management", SANS Institute, online at www.sans.org/reading_room/whitepapers/auditing/introduction-information-system- risk-management_1204

[4] Murray, R. and Hillson, D. (2008) Managing group risk attitude, Gower Publishing Ltd.

[5] Kajko-Mattsson K. and Nyfjord J., (2008) "State of Software Risk Management Practice", IAENG International Journal of Computer Science, Vol. 35, No. 20

[6] APM (1997) "Association for Project Management Project Risk Analysis and Management Guide (PRAM Guide)", APM Risk Specific Interest Group

[7] PMI (2000) Project Management Institute Guide to the Project Management Body of Knowledge (PMBOK)

[8] Kloman, H.F. (1990) "Risk management Agonistes", Risk Analysis, Vol. 10, No. 2

[9] Mills, K. and Walle, B. (2007) "IT for Corporate Crisis Management: Findings from a Survey in different Industries on Management Attention, Intention and Actual Use", Proceedings of the 40th Hawaii International Conference on System Sciences – 2007, pp 24, January, Hawaii

[10] Spillan, J.E. and Hough, G.M. (2005) "Crisis Planning: Increasing Effectiveness, Decreasing Discomfort", Journal of Business and Economics Research, Vol. 3, No. 4, pp. 19-24 Standish Group (1994) CHAOS Report, The Standish Group, USA

[11] Latto, A. (2007) Managing risk from within: monitoring employees the right way, Cengage Learning, Gale, USA

[12] Mitroff, I., Pauchant, T., Finney, M. and Pearson, C. (1989) "Do some organisations cause their own crises? The Cultural profiles of crisis-prone vs. Crisis-prepared organisations", Industrial Crisis Quarterly 3, pp. 269 – 283

[13] Higuera, R.P. and Haimes, Y.Y. (1996) Software Risk Management: Technical Report, Carnegie Mellon University, Pennsylvania

[14] Gibson, M. (1997), "Information systems for risk management: Federal Reserve Board", online at www.bis.org/publ/ecsc07f.pdf

[15] Wallis, M.R., (2005), "Corporate risk taking and performance", online at pages.stern.nyu.edu/~adamodar/pdfiles/papers/strategicrisk.pdf

[16] Twain, M. (2010) Project Risk Management, online at www.wsdot.wa.gov/publications/fulltext/cevp/ProjectRiskManagement.pdf