

A Novel Methodology for the Impact Measurement of Reengineering Risk in Infrastructure and Stakeholder Segment of Legacy System

Anand Rajavat

Department of Computer Science & Engineering
Shri Vaishnav Institute of Technology and Science
Indore, M. P., India

Vrinda Tokekar

Department of Information Technology
Institute of Engineering and Technology (DAVV)
Indore, M. P., India

ABSTRACT

Successful reengineering effort requires identifying and measuring impact of various risk components of legacy system. Risk identification and measurement process involve a clear understanding of various legacy system segments in accordance with requirements of target system. In this paper we pay attention to infrastructure and stakeholder segment of legacy system. We identify and measure impact of different risk components related to infrastructure and stakeholder segment of legacy system. In infrastructure segment we cover risk components and affecting factors associated with system development & deployment process of organization and its available resources. In the stakeholder's segment we addresses risk components and affecting factors related to personal and professional attributes of stakeholders involve in reengineering process of legacy system. Finally, we contribute to analyze the cause-effect relationship between the reengineering process and existing state of legacy system in accordance with requirements of target system.

Keywords

Reengineering, Risk, Legacy system, Risk measurement, Organization

1. INTRODUCTION

Legacy systems [1-3] were developed before the widespread use of modern software engineering methods [4-5]. Keith Bennett provides some useful parameters for identifying a legacy system like age (more than 10 years old), the size (hundreds of thousands of lines of code), an old coding language (assembly or an early version of a third generation language), a long history of maintenance, maintenance costs, significance of the mission and the encapsulated domain knowledge [6-7]. However some new systems may also considered legacy because of the weak technology employed, even when they have been recently developed [8-10].

Reengineering offers an approach to migrate a legacy system towards an evolvable system in a disciplined manner. The goal of software re-engineering is to take an existing software system and generate from it a new system that has the same quality as software created by modern software engineering practices [11]. The reengineering problems and their influence on software quality make software re-engineering process complex. As an engineering problem reengineering also requires quantitative analysis of the different problems and consideration of reengineering risks in its solution. Therefore we need to consider a broad range of

risk issues and concerns to understand and model successful re-engineering process.

In this paper we cover organizational infrastructure and stakeholder segment of legacy software system. We identify and measure impact of various risk components of that segments. We also analyse effect of risk impact on reengineering process of legacy software system. For each segment we include five different risk components and develop corresponding risk impact measurement mechanism. We also identify critical risk measures of each risk components of infrastructure and stakeholder segment of legacy software system.

2. LITERATURE SURVEY

To simplify the problems of replacing legacy systems an organization may decide to reengineer these systems and improve their structure and understand ability. Reengineering rapidly replace legacy development for keeping up with ever-evolving business and user requirements. Gang Zhangl in [12] analyze major components of reengineering process qualitatively and quantitatively by considering some important factors such as investment, style of investment, returns on investment and quality. Authors in their study develop incremental and iterative process by considering needs of stakeholders. They also establish an incremental and iterative process framework and a series of work steps and guidelines to increases reengineering success in a cost effective manner.

Paulo Cesar Masiero in [13] uses software patterns to reengineering legacy system in the direction of simplify the reengineering process and improving future maintenance. The approach has three steps: apply reverse engineering, recognize software patterns present in the object model obtained and re-implement the system in a more productive way. Proposed method delimited components and larger chunks of design to be reused as a whole or as part.

Boehm proposed a risk-driven software development model. The strength of this model is to eliminate risks from the early stages of software development, instead of encountering project barriers at the later stages. Boehm extended his original spiral model using the theory of Win-Win Model (Boehm and Ross, 1988; Boehm and Bose, 1994). The Win-Win Model also supports risk identification, resolution, and continuous monitoring of risks. Boehm (1991) also proposed a risk management framework, which helps to identify the primary sources of risk, analyze and resolve them. This risk management framework can be integrated into the Original Spiral, or the Win-Win Model [14].

Misra et al. have proposed an approach for software engineering risk management. This approach could be used by

project managers to model, and control risks in software projects. The approach is helpful to project managers for performing means-end analysis, thereby uncovering the structural origin of risks in a project, and how the root-causes of such risks can be controlled from the early stages of the projects [15].

3. INFRASTRUCTURE SEGMENT

All Organizations require a high level development approach when they adopt a reengineering effort. However due to unfinished organizational standards and policies for the management of various stakeholders and resources reengineering approach lose its focus. Infrastructure segment focuses on availability of organizational resources, and its project development structure and practices. It also describes existing state of organization by analyzing infrastructure support they provide, the process they used and the work product they produce to support target system requirements. We describe following five risk components and relative impact measurement mechanism for infrastructure segment of legacy software system [16].

3.1 Organizational Risk Component

Organizational risk component represent the loss resulting from inadequate or failed internal organizational structure, undefined objectives & values, complex development processes and uncertainty in the organization's activities.

- **Impact Measurement Mechanism**

In organizational risk measurement mechanism we measure organizational structure, development approach as well as objectives and values (personal and cultural) of the organization maintaining the legacy system, to support decision making process for reengineering. We identify and scale several measures as shown in table 1 that will affects impact value of organizational risk component [17].

Table 1 Measures of Organizational Risk Component

S. No.	Measure	Scale value Yes-1 No-0
1	Quantitative overload	
2	Role conflict and ambiguity	
3	Less involvement in decision making process	
4	Unhealthy physical environment and working conditions	
5	Excessive work schedules	
6	Lack of recognition policy	
7	Complex interpersonal relations	
8	Obscure information flow	
	Total Scale value (X)	

In Table 1 we represent measures and relative scale value used to compute total scale value of organizational risk component. Once we have identified the measures, a measurement metrics represented by equation 1 is used to compute impact of organizational risk component (TIOR). First we calculate impact of each measure by using a scale value that represents to what extent user of legacy system and developer of target system agree or disagree for respective measure. We use a scale of 1 for yes and 0 for no answer then we can get the scale value for each measure by looking at the answers given by users of legacy system and developers of target system. The average value is used to assign scale for each measure for more than one answer.

$$TIOR = \frac{\sum_{i=1}^N (X)}{N} \quad (1)$$

Where, TIOR represents total impact of organizational risk, X represents scales value of measures given by legacy system users and developers of target system and N represent number of measures.

3.2 Resource Risk Component

Resource related risk is defined as the risk of loss due to the low quality resource, resource unavailability or delayed resource availability to support system evolution activity. Unavailability of required information such as analysis and design documents of existing legacy system will affect impact of resources related risk. Improper estimation of required resources for the reengineering of legacy system also increases impact of resources risk component [18].

- **Impact Measurement Mechanism**

In resource risk measurement mechanism we measure availability and quality of resources. We consider a variety of resources including hardware, software, human and reusable components in accordance with the available budget, schedule and strategic objectives of reengineering of legacy system. We express resource availability for system evolution as the period during which a selected resource is required. The duration can be continuous or it can be divided into separate segments, depending on the requirements of system evolution task. We measure Total Risk Impact (TRI) value of resource risk component using equation 2.

$$TIRER = \frac{[\text{No.of resources unavailable}]}{\text{Total no.of resources required for target system}} \quad (2)$$

Where TIRER represents total impact of resource risk

3.3 Deployment Risk Component

Deployment risk component indicate the loss associated with uncomfortable structure of existing organization to support deployment requirement of target system. Unsupportable organizational infrastructure to satisfy minimum deployment and maintenance requirement of target system increases the impact of deployment risk component [19].

- **Impact Measurement mechanism**

The successful deployment of a target system is an important issue in legacy system evolution. However it is critical that the deployment is achieved successfully with minimal disruption to current production services. We found that to ensure this we required to measure deployment risk component. We develop a deployment risk assessment worksheet to quantify Total Risk Impact (TRI) value of deployment risk component. The deployment risk assessment worksheet analyzes the availability of elements that need to be in place before the deployment of target system.

In table 2, 3 and 4 we represent elements of application section, Infrastructure section and Support section.

Table 2 Elements of Application Section

S. No.	Elements	Scale value [Y=1,N=0]
1	Feedback from previous test implementations are unavailable	
2	Unavailability of technical details of legacy application.	
3	Load and scalability testing is required for enhanced application	
4	Performance has not been assured by user and support testing staff.	
5	The details regarding new infrastructure components have been added to the configuration management database.	
6	No change control entry has been created for the legacy application.	
7	Contradictory Database environment between legacy and target system.	
8	Are there any new technologies involved?	
Total scale value (TSV)		

Table 3 Elements of Infrastructure Section

S. No.	Elements	Scale value [Y=1,N=0]
1	Legacy system architecture and target system architecture are different	
2	Security requirements, e.g. SSL encryption, IP based restrictions firewall are mandatory	
3	Amended infrastructure is included in evolving process.	
4	New hardware required as part of the project evolution process.	
Total scale value (TSV)		

Table 4 Elements of Support Section

S. No.	Elements	Scale value [Y=1,N=0]
1	Need for support agreement for new applications – including any hosting or support charges.	
2	Required system description documents are not available	
3	Predetermined schedule for evolution task	
4	Backup requirement is mandatory	
5	Required licensing is unprepared including maintenance/support arrangements with external suppliers.	
6	The new application requires helpdesk.	
7	System operational documentation required for users of the new application.	
8	Operational Training required for existing users.	
9	Demonstration or walkthrough of new application for other stakeholder.	

S. No.	Elements	Scale value [Y=1,N=0]
Total scale value (TSV)		

Once we measure Total scale values for application, infrastructure and support sections, we compute Total Risk Impact (TRI) value for deployment risk component using equation 3.

$$TIDR = \frac{\sum_{i=1}^N (TSV)}{N} \quad (3)$$

Where, TIDR represents total impact of deployment risk, N represent no. of sections and Total Scale Value (TSV) for each section represents average of assigned scale value for elements of different sections.

3.4 Development Process Risk Component

Development process risk component defines the risk as a loss associated with undefined objectives of development process and inadequate management of various development process elements (human, physical and financial elements). For a successful reengineering effort there is a need to establish an effective development process which defines a set of task and guidance to perform each task [20].

• Impact Measurement Mechanism

In development process risk measurement model we measure various elements of development process involve in reengineering process of legacy system. For the identification of development process risk we require objectives of organization with optimum combination of human, physical and financial resources.

Defect Removal Effectiveness is an important metrics to measure development process risk component. Defect removal effectiveness can be defined using equation 4.

$$DRE = \frac{\text{No.of defects removed during development phase}}{\text{Defects latent in the product}} \quad (4)$$

Because the total number of latent defects in the product at any given phase is not known, the denominator of the metric can only be approximated. It is usually computed using equation 5.

$$\text{Defects latent} = \text{No. of defects removed during the development phase} + \text{No. of defects found later} \quad (5)$$

The metrics can be calculated for the entire development process, for the front end, and for each phase of software development life cycle. Once we have computed DRE value of existing development process we measure Total Risk Impact (TRI) value for development process risk component using equation .6.

$$TIDPR = 1 - \frac{\sum_{i=1}^N DRE}{N} \quad (6)$$

Where, TIDPR represents total impact of development process risk, DRE represents Defect Removal Efficiency and N represents no. of software development life cycle (SDLC) phases.

3.5 Reusability Risk Component

Reusability risk components represent the loss associated with insufficient availability of reusable artifacts used to develop target system requirements. The impact of reusability risk component depends on the extent to which different artifacts

of legacy software system can be reused in the development of target system [21].

- **Impact Measurement Mechanism**

Reusability is an important issue in reengineering process of legacy software system. The cost effectiveness of any reengineering task depends on the extent to which different artifacts which includes architecture, requirements, design, project management plans, user manuals and source code of existing legacy system can be reused in target system. If only source code is reused, the benefits of reengineering will be marginal. Optimal reengineering benefits occur only when reusability spans all the major software artifacts. Reusability risk measurement mechanism analyzes legacy system to identify number of reusable artifacts in accordance with requirements of target system. Equation 7 is used to compute Total Risk Impact (TRI) value of reusability risk component.

$$\text{TIRUR} = \frac{[\text{No. of nonreused software artifact}]}{\text{Total no. of software artifacts required for target system}} \quad (7)$$

Where

TIRUR represents total impact of reusability risk component.

4. STAKEHOLDER SEGMENT

Most of the organizations have a long –range strategy when they embark on a reengineering effort. However these strategies may be seriously flawed or incomplete due to lack of attention to the various attributes related to the stakeholder's involved in reengineering. In stakeholder segment we cover user and developer's thinking towards reengineering as a system evolution strategy. We also analyze roles and responsibility of stakeholders for a particular organization. We address various issues like team organization, communication strategy, personal comfort ability and user's skill set in the context of stakeholder segment. To consider these issues we identify five different risk components of stakeholder segment [22].

4.1 Team Risk Component

A team that is not working can cause unnecessary disruption, failed delivery and strategic failure. Measurement of team risk component in the reengineering process of legacy system involves some key measures that will affect overall impact of team risk component. Team risk component defines the risk of loss associated with complex team structure and unproductive activities of evolution team [23].

- **Impact Measurement Mechanism**

In team risk measurement mechanism we measure team-oriented activities of customer and developer. For the identification of team risk we require to consider shared product vision, target results, and objectives of organization. We identify and measure attributes of organizational structure and operational activities.

Teamwork has a dramatic effect on organizational performance. An effective team can help an organization to achieve incredible results. Measurement of team risk component in the reengineering process of legacy system involves some key measures that will affect overall impact of team risk component. We investigate some important measures and corresponding scale values shown in table 5.

Once we have identified the measures and assign scale value to each measure a mean opinion score board as represented in table 6 is used to check team effectiveness and relative Total Risk Impact (TRI) value of team risk component.

Table 5 Measures of Team Risk Component

S. No.	Measures	P	A	S	G
Scale Value		0	1	2	3
1	knowledge level of team members about the stages of development process				
2	Feedback system regarding performance of team members				
3	Encouragement of team members to work for the common goal of the organization.				
4	Understanding of team members about decisions				
5	Policy effectiveness for stakeholder's encouragement to be good team members, and build good relationships.				
6	Development opportunities for team members				
7	Chances for team members to work on interesting tasks and stretch their knowledge and capabilities.				
8	Understanding of team members on requirements and the resources needed to accomplish those requirements successfully.				
9	Reward policy for good work				
10	Working relationships & coordination across units or functions				
Total					

Where P represents poor, A represents average, S represents satisfactory and G represents good scale values.

Table 6 Mean Opinion Score for Team Risk Component

Score	Comment	Total Impact of Team Risk (TITR)
20-30	Solid team, member working well as part of an effective team.	0 Minimum
10-19	Team effectiveness is patchy. Team is good at some things, but there's area for improvement.	0.5 Average
00-09	Unconfident team structure and poor team effectiveness	1 Maximum

4.2 Communication Strategy Risk Component

Effectiveness of communication strategy depends on process of information exchange as well as opinion of individuals on communication process. The loss associated with communication gap and communication conflicts between various stakeholders involved in reengineering process of legacy system is consider as communication strategy risk [24].

• Impact Measurement Mechanism

In communication strategy risk measurement mechanism we measure, process for exchange of information as well as opinion of individuals, groups, and organization on communication process. Identification of communication strategy risk consider medium and approach of communication. We also identify different causes of communication gap between stakeholders involve in reengineering process of legacy system. We need to highlight more clearly the nature of the communication conflict. Identification and resolution of communication risk is implicit in the reengineering task since it requires effective and proper communication between stakeholders of legacy and target system.

We identify and use some key measures as shown in table that will affect overall impact of communication strategy risk component. With the help of table 7 we represent measures and corresponding scale value for communication strategy risk component.

Table 7 Measures of Communication Strategy Risk Component

S. No.	Measure	Scale value [Y=1 N=0]
1	Data and information needed to evolve legacy system is	

	unavailable	
2	Disparity in characteristic of a person involve in the communication process	
3	Undefined medium for communication between stakeholders	
4	Poor communication skills of existing users	
5	Undefined organizational communication policy and rules	
	Total scale value (X)	

Once we have identified the measures and corresponding scale values for that measures a measurement metrics represented by equation 8 is used to compute Total Risk Impact (TRI) value of communication strategy risk component. We are able to compute impact of each measure by using a scale value that represents to what extent user of legacy system and developer of target system agree or disagree for respective measure. If we use a scale of 0 (strongly agree) to 1 (strongly disagree) then we can get the scale value for each measure by looking at the answers given by user of legacy system and developer of target system. The average scale value is used to assign scale for each measure for more than one answer.

$$\text{TICSR} = \frac{\sum_{i=1}^N (X)}{N} \quad (8)$$

Where TICSR represents total impact of communication strategy risk component, X represents total scale value and N represent number of measures

4.3 Personal Risk Component

Personal attributes includes job matching, team building, moral building, work schedule, as well as communication and financial aspects of system evolution at personal and organizational level. Personal risk component express the loss related with uncomfortability of personal (user and developer) with the system evolution objectives [25].

• Impact Measurement Mechanism

In personal risk measurement model we identify and measures comfort ability of personals both users of legacy system and developers of target system in accordance with objectives of reengineering. We identify and define job matching, team building, moral building, schedule, communication and financial aspects of system evolution at personal and organizational level as follow.

Table 8 Measures of Personal Risk Component

S. No.	Measure	Scale value [Yes = 1 No = 0]
1	Dissatisfied Job matching	
2	Complex team building state	
3	Unavailability of moral building process	
4	Uncomfortability with evolution schedule	
5	Poor communication skill level	
6	Unsatisfied financial aspects	
	Total Scale Value (X)	

In table 8 we represent key measures and corresponding scale values given by user of legacy system and developer of target system. Once we have identified the key measures a measurement metrics shown in equation 9 is used to compute Total Risk Impact (TRI) value for personal risk component. First we compute impact of each measure by assigning a scale value that represents to what extent user of legacy system and developer of target system agree or disagree for respective measure. We use a scale of 1 for yes and 0 for no answer for each measure by looking at the answers given by user of legacy system and developer of target system. The average scale value is used to assign scale for each measure for more than one answer.

$$TIPR = \frac{\sum_{i=1}^N (X)}{N} \quad (9)$$

Where TIPR represents total impact of personal risk component, X represents scale value given by legacy system users and developers of target system and N represent number of measures

4.4 User Risk Component

User risk component is the risk due to the lake of user involvement during system evolution process. If the attitude of users toward a new system is unfavorable they will not cooperate during reengineering effort, leading to an increased risk of project failure [26].

• Impact Measurement Mechanism

With the help of user risk measurement mechanism we identify and measure user associated risk factors. We consider user resistance to change, lake of cooperation from users, conflict between users, unattainable users commitment and negative attitude of stakeholders towards the evolution task.

User involvement is often assumed to be a key for successful reengineering. However, few empirical studies have clearly demonstrated a relationship between user involvement and two key indicators of system success: system usage and user satisfaction. System evolution task emphasized the need to undertake user involvement activities in a systematic way. In table 9 we demonstrate nine dimensions of user involvement. An assessment can be made for each criterion according to the weight presented in table 9.

Table 9 Dimensions of User Involvement

S. No.	Dimension	Weighting Factor
1	Aims and scope of user involvement	
2	Systematic approach to user involvement	
3	Resources for user involvement	
4	Information and communication	
5	Training and support	
6	Representation and inclusion	
7	Power and control	
8	Evidence of change	
9	Feedback and follow-up	

We use a set of criteria to evaluate present user involvement system. Within user involvement system we consider a range of different elements of user involvement to evaluate existing user involvement process.

Table 10 Assessment of User Risk Component

Assessment Measure	Weight
Has no plans to develop this element	1
Is currently developing this element	0.5
Already has this element in place.	0

Once we have identified the dimensions of user involvement and assign corresponding weight for each dimension, we develop a measurement metrics shown in equation 10 to compute Total Risk Impact (TRI) value of user risk component

$$TIUSR = \frac{\sum_{i=1}^N (X)}{N} \quad (10)$$

Where, TIUSR total impact of user risk, X represents total weighting factor and N represent number of measures

4.5 Specialization Risk Component

Identification and measurement of specialization risk requires to consider several risk factors which includes job matching, experience, skill level, schedule, organizational change policy, administration & financial support as well as user perceptions for system evolution task at personal and organizational level. Specialization risk component represents the risk associated with inexperience and amateur workforce for system evolution task [27].

- **Impact Measurement Mechanism**

During specialization risk measurement mechanism we measures technical and development skills and experience of the software developers involve in reengineering process. For the identification and measurement of specialization risk we need to consider expertise and experience of developers on basic tools and technology that was used in development of legacy system as well as advanced tool and technology which will be use to achieve goals of desired target system. Key measures used to compute impact of specialization risk component are shown in table 11.

Table 11 Measures of Specialization Risk Component

S. No.	Measure	Scale value [Yes = 1 No = 0]
1	Developers have no reengineering experience	
2	Developers are incompetent in required technology skill level for target system	
3	Incompatible development Schedule	
4	Lack of organizational training policy for targeted system	
5	Developers poor Communication Skills	
6	Unsupportive administration support	
7	Weak financial support	
8	Poor user perceptions towards reengineering	
	Total Scale Value (X)	

Once we have identified the measures and corresponding scale value of measures a measurement metrics is developed to compute Total Risk Impact (TRI) value of specialization risk component. Impact of each measure can be calculated by using a scale value that represents to what extent user of legacy system and developer of target system agree or disagree for respective measure. If we use a scale of 0 (strongly agree) to 1 (strongly disagree) then we can get the scale value for each measure by looking at the answer given by user of legacy system and developer of target system. Finally total impact of specialization risk component can be computed using equation 11.

$$TISR = \frac{\sum_{i=1}^N (X)}{N} \quad (11)$$

Where, TISR represents total impact of specialization risk component, X represents scale value given by legacy system

users and developers of target system and N represent number of measures.

5. CONCLUSION

Successful reengineering improves quality of legacy system for the satisfaction of all the stakeholders. However reengineering risk and their influence on software quality causes reengineering efforts to fail. Development of successful reengineering effort required to manage such reengineering risks. In this paper we focus on infrastructure and stakeholder segment of legacy system. We first identify several risk components related to these segments. A variety of measurement mechanisms are developed to measure impact of each risk components of infrastructure and stakeholder segment of legacy software system.

6. REFERENCES

- [1] Brodie M.L., Stonebraker M., "Migrating Legacy Systems: Gateways, Interfaces & the Incremental Approach," Morgan Kaufmann Publishers, Inc., San Francisco (1995).
- [2] Dajsuren Y., "Modernizing Legacy Software Using a System Grokking Technology," published in IEEE International Conference on Software Maintenance (ICSM), 2010.
- [3] Pérez-Castillo, R., "Process Mining through Dynamic Analysis for Modernizing Legacy Systems," paper appears in Software, IET, and volume: 5, Issue: 3, PP: 304 – 319, June 2011.
- [4] Jelber, Sayyad, Shirabad, "Mining the Maintenance History of a Legacy Software System," published in Proceedings of International Conference on Software Maintenance, PP 95 - 104 2003. ICSM 2003.
- [5] Breivold, H.P., "Analyzing Software Evolvability", published in 32nd Annual IEEE International conference on Computer Software and Applications, PP: 327 - 330 2008. COMPSAC '08.
- [6] Wu, B.H., "On Software Engineering and Software Methodologies A Software Developer's Perspective," Published in International Conference on Information Science and Technology (ICIST), PP 155 - 162, 2011.
- [7] Hamou-Lhadj A., " The Impact of the Model-Driven Approach to Software Engineering on Software Engineering Education," Published in Sixth International Conference on Information Technology: New Generations, PP: 719 - 724 2009. ITNG '09.
- [8] Clarke, J., "Reformulating Software Engineering as a Search Problem," appears in Software, IEEE Proceedings - Volume: 150, Issue: 3 PP: 161 - 175, June 2003.
- [9] Mills H. D., "The management of software engineering, Part I: Principles of software engineering", appears in: IBM Systems Journal, Volume: 19, Issue: 4, PP: 414 – 420, 1980.

- [10] Keith Bennett, "Legacy Systems: Coping with Success," Published in Journal IEEE software volume 12 Issue 1 January 1995, PP 19-23 , IEEE Computer Society Press Los Alamitos, CA, USA.
- [11] Santiago Comella-Dorda, Kurt Wallnau, Robert C.seacord, John Robert, "A Survey of Legacy System Modernization Approaches," Technical Note, CMU/SEI-20000-TN-003.
- [12] Gang Zhang1, Liwei Shen1, Xin Peng1, Zhenchang Xing2, Wenyon Zhaol," Incremental and Iterative Reengineering towards Software Product Line: An Industrial Case Study", 27th IEEE International Conference on Software Maintenance (ICSM), 2011.
- [13] Paulo Cesar Masiero, "Legacy Systems Reengineering Using Software Patterns," Published in Proceeding of SCCC '99 Proceedings of the 19th International Conference of the Chilean Computer Science Society IEEE Computer Society Washington,DC, USA ©1999, table of contents ISBN: 0-7695-0296-2, PP: 160, 1999.
- [14] Boehm B.W., "Software Risk Management: Principles and Practices," IEEE Software, Volume 8, Issue 1, PP.32 – 41, 1991.
- [15] Subhas C. Misra, "Different Techniques for Risk Management in Software Engineering: A Review," ASAC -2006, and PP: 196-205, 2006.
- [16] Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "A Quantitative Model for the Evaluation of Reengineering Risk in Infrastructure Perspective of Legacy System" published in IEEE CSI 6th International Conference on Software Engineering CONSEG – 2012
- [17] Tang Yong, "The Analysis of Organizational Risk-bearing Capability in the Uncertain Environment," appears in International Conference on E-Business and E-Government (ICEE), PP: 4720 - 4723 2010.
- [18] Wen-Hsien Tsai,Sin-Jin Lin ; Jau-Yang Liu ; Kuen-Chang Lee ; Wan-Rung Lin ; Jui-Ling Hsu, " Examining the Implementation Risks Affecting Different Aspects of Enterprise Resource Planning Project Success," appears in 40th International Conference on Computers and Industrial Engineering (CIE), PP: 1 - 6 ,2010.
- [19] Tang Dan, Kuang Xiao-Hong, "Risk Management, Centralized EIP System Upgrade Deployment," appears in IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, PP: 150 - 153 2008.
- [20] Chun-Hui Wu, "Exploring Impacts of Software Development Process Maturity on Project Risk," appears in IEEE International Conference on Industrial Engineering and Engineering Management, PP: 1033 - 1037, 2008. IEEM 2008.
- [21] Jag Sodhi, Prince Sodhi,,"Software Reuse-Domain Analysis and Design Process," McGraw-Hill, ISBN 0-07- 0579237.
- [22] Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "Decision Driven Risk Measurement Model to Quantify Reengineering Risk in Stakeholder Perspective of Legacy System" Registered in IEEE Ninth International Conference on Wireless and Optical Communications Networks WOCN2012.
- [23] Chun-Hui Wu, Kwoting Fang, "The Impact of Organizational Learning on Lack of Team's Expertise Risk in Information Systems Projects," appears in IEEE International Conference on e-Business Engineering, 2007, PP: 738 - 743, ICEBE 2007.
- [24] Jiang Rong ,Liao Hongzhi ; Yu Jiankun ; Feng Tao ; Zhao Chenggui ; Li Junlin, " A Model Based on Information Entropy to Measure Developer Turnover Risk on Software Project," appears in 2nd IEEE International Conference on Computer Science and Information Technology, 2009. PP: 419 - 422 ICCSIT 2009.
- [25] Dr. Thomas Fehlmann, "Metrics for Cooperative Development Processes," Euro Project Office AG, Zurich, Switzerland, IWSM/MetriKon 2004.
- [26] Panko, R.R, "Minitrack on Risks in End User Computing," appears in Proceedings of the Twenty-Ninth Hawaii International Conference on System Sciences, Volume: 2 1996.
- [27] Shazia Mumtaz, "Factors Affecting Teachers' Use of Information and Communications Technology: A Review of the Literature," Journal of Information Technology for Teacher Education, University of Warwick, Coventry, USA, 2006.