A Quantitative Model for the Evaluation of Reengineering Risk in Infrastructure Perspective of Legacy System

Er. Anand Rajavat
[1]Department of Computer Science & Engineering
SVITS, Indore, M. P., India
anandrajavat@yahoo.co.in

Dr. (Mrs.) Vrinda Tokekar
Information Technology
IET (DAVV), Indore, M. P., India
Vrindatokaker@yahoo.co.in

ABSTRACT

Competitive business environment wants to revolutionize existing legacy system in to self-adaptive ones. Nowadays legacy system reengineering has emerged as a well-known system renovation technique. Reengineering rapidly replace legacy development for keeping up with modern business and user requirements. However renovation of legacy system through reengineering is a risky and error –prone mission due to widespread changes it requires in the majority of case. Quantifiable risk measures are necessary for the measurement of reengineering risk to take decision about when the modernization of legacy system through reengineering is successful. We present a quantifiable measurement model to measure comprehensive impact of different reengineering risk arises from infrastructure perspective of legacy system. The model consists of five reengineering risk component, including Deployment Risk, Organizational Risk, Resource Risk, Development Process Risk and Personal Risk component. The results of proposed measurement model provide guidance to take decision about the evolution of a legacy system through reengineering.

Keywords
Reengineering, Risk Engineering, Measurement.

I. INTRODUCTION

Economic and political conditions of software business environment have grown multifold in the last couple of decades. Expectation levels of market and users grow in rapid succession. Software organizations are continually attempting numerous rising challenges for effective development process and ensure production of high quality product.

In the course of the last years, an ever increasing amount of software systems have been built and used. In the meantime innovation cycle of software technology changed dramatically .Therefore all software which has been developed without using the most current technology is considered legacy system.

Legacy systems [1] were developed before the widespread use of modern software engineering [2] [3] methods and have been maintained to accommodate changing business and user requirements. Most of the legacy systems we use have complex design structure have inefficient coding and incomplete documentation. Modernizing legacy system to meet continual changing user and business needs is difficult. A legacy system may evolve in a number of ways, depending on factors such as its technical condition, its managerial value and the characteristics of the organization involved in maintaining and operating the system. Continued maintenance, reengineering and replacement are the general evolution strategies of which one or a combination may be an appropriate way of evolving a legacy system. [4]

Now a days software reengineering is becoming more widely implemented to reengineer legacy systems to make them more maintainable. Software re-engineering are concerned with maximizing software usage for any given development effort. Reengineering [5] [6] strategy includes: reverse engineering, restructuring, translation, data reengineering, redocumentation, forward engineering and retargeting. Reengineering of programs and data of legacy system reduces the overall development cost and time. However research shows that different risk component of reengineering process and their impact on software quality causes reengineering efforts to fail. A practicable re-engineering process required to measure overall impact of different reengineering risk components engenders from system, managerial and technical domains of legacy system [7].

Proposed work measures total impact of various risk components concerned with infrastructure perspective of legacy system. We first estimate risk impact of individual risk component for infrastructure perspective of ReeRisk framework [4]. Different measurement metrics is used to measure impact of specific risk component in reengineering process. Finally a pentagram model [8] is used to compute comprehensive impact of all the risk components. The Infrastructure perspective of ReeRisk framework consists of five reengineering risk component, including Deployment Risk, Organizational Risk, Resource Risk, Development Process Risk and Personal Risk component.

II. RELATED WORK

Measurement is an important phenomenon of any engineering discipline. As with any engineering discipline, software reengineering also requires efficacious measurement mechanism to make better decisions based on facts and information. A proper risk

measurement process will increase success rate of designated evolution strategy used to modernize any legacy system. Measurement allows us to determine the strengths and weaknesses of the legacy system for the successful completion of software reengineering process.

Svensson in [9] define differences between the two research methodologies. According to them, the quantitative method tries to find answers by searching for similarities through statistical evidence. The qualitative research on the other hand seeks answers by researching different features of the single object. On the other side P.K. Suri in [10] provide a quantitative means to assess the risk associated with software development, by outlining the different factors which introduce the risk, assigning weightages to each factor , calculating the overall risk score and then categorizing the project risk as low , medium, high or extreme. Kishor S. Trivedi in [11] presents a stochastic model to measure the effectiveness of proactive fault management in software systems and determine optimal times to perform rejuvenation, for different scenarios. Model develops different methodologies to detect software aging and estimate its effect on various system resources. Whereas Paul R. Garvey in [12] suggest how individual technical performance measures may be combined to measure and monitor the overall performance risk of a system.

The existing legacy system assessment models really measure risk impact by considering current state of legacy system and desired state of target system. The current methods to measure the reengineering risk usually focused on a particular perspective of legacy system. However overall risk measurement requires considering system, managerial and technical domain of legacy system. Successful reengineering requires decision driven model for the identification and measurement of different risk components, and calculating overall impact score of all risk components.

III. INFRASTRUCTURE PERSPECTIVE RISK MEASUREMENT MODEL

The purpose of infrastructure perspective risk measurement model is to design quantifiable metrics for the evaluation of legacy system. Model measures impact of different reengineering risk components materialize in the evolution process of legacy system. As a final point model is able to design mean opinion score board to support decision making process.

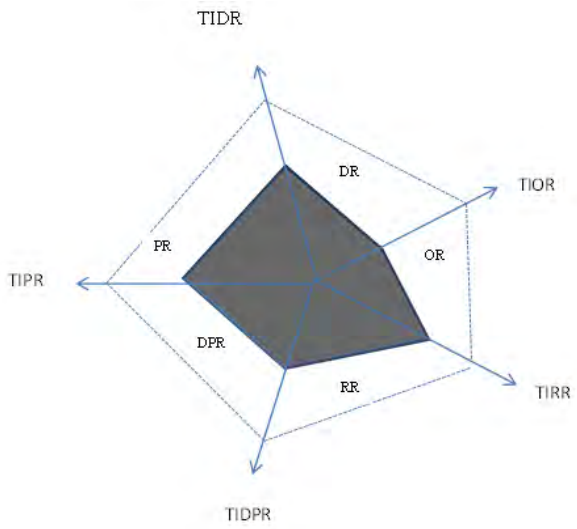

Figure 1 INFRASTRUCTURE PERSPECTIVE PENTAGRAM MODEL

As shown in Figure 1 infrastructure perspective measurement model is presented using a pentagram diagram based on the measurement of its five risk components. The total impact of each risk component is measured based on the results of their metrics during measurement process [13] [14].Let us assume: the measurement results of each risk component is a value from 0 to 1. The value "1" indicates the maximum value for each risk component, and "0" indicates the minimum value. The area of the pentagram is used as the measurement of overall impact of five risk components. Clearly, the smallest value of this pentagram area is 0, and the maximum value is approximately 2.4. As the pentagram consists of five triangles, the area of each triangle can be computed $0.5 * L1 * L2 * \text{Sin}\alpha$ where L1, L2 represent the sides of the triangle and α represents the 72-degree angle between the two sides. The term TIDR, TIOR, TIRR, TIDPR, and TIPR in Figure 1 are used to represent the five risk components of model respectively. Since each risk component is measured using different quantifiable measurement metrics the Total Risk Impact (TRI) of all risk components from infrastructure perspective of legacy system can be computed as below:

$$\text{P1-Total Risk Impact (TRI)} = 1/2 \text{ Sin } 72\ (ab + bc + cd + de + ea)$$

$$= \tfrac{1}{2} \text{ X } 0.9511\text{X}(ab + bc + cd + de + ea)$$

$$= 0.48 \text{ X } (ab + bc + cd + de + ea)$$

Where a represents TIDR, b represents TIOR, c represents TIRR, d represents TIDPR, e represents TIPR.

Infrastructure perspective pentagram model is used to measure overall impact of five different reengineering risk components from the infrastructure point of view of organization running legacy system. The five most important risk components of infrastructure perspective

are presented in Table I. It shows Key risk component and the most important measures of those components. Infrastructure perspective risk measurement is designed using a pentagram model to measure total impact of different reengineering risk components in infrastructure perspective of legacy system.

Table 1 Most Important Measure

Key Risk component	Most Important Measures	Symbol
Deployment Risk Component	1. Application purview 2. Infrastructure purview 3. Support purview	a
Organizational Risk Component	1. Quantitative overload, qualitative overload 2. Role conflict and ambiguity 3. Participation in decision making process 4. Physical environment and working conditions 5. Work schedules 6. Recognition 7. Interpersonal relations 8. Information Flow	b
Resource Risk Component	1. No: Number of Resources 2. AVG: Average Cost per Time Unit 3. SUM DUR: Total Duration 4. SUM COST: Total Cost per Time Unit 5. AWH :Annual Working Hours 6. AC :Annual per Time Unit Cost	c
Development Process Risk Component	1. Defect removal effectiveness 2. Customer Needs analysis, including Kano prioritization 3. Quality Function Deployment into solution characteristics and product features (Design for Six Sigma) 4. Progress Metrics for project planning and tracking 5. Deliverable Sizing 6. Metrics for test prioritization and evaluation 7. Bug metrics	d
Personal Risk Component	1. Job Matching 2. Team building 3. Moral building 4. Schedule aspects 5. Communication Skill 6. Financial aspects	e

IV. MEASUREMENT METRICS

In this section, we describe the measurement metrics used to measure impact of each risk component represented by each side of the pentagram model.

- *Deployment Risk Component*

Deployment risk component is the risk of loss associated with present structure of organization to support deployment of target system. Deployment risk measurement model measures the present organizational structure with the view of target system deployment. Identification and measurement of deployment risk requires to consider organizational operational environment, organizational structure, network capability, hardware, and software support and user skill level.

The deployment of a target system is a significant milestone in the evolution process of legacy system. However it is critical that the deployment is achieved successfully with minimal disruption to current production services. To ensure this it is required to measure deployment risk component. The Deployment risk assessment worksheet is an important metrics to quantify total impact of deployment risk component. The deployment risk assessment worksheet highlights the key elements that need to be in place before the deployment of target system [15].

Deployment risk assessment worksheet involves three sections presented by tables 2, 3 and 4 and final score board shown in table 5.

- Application purview
- Infrastructure purview
- Support purview

Table 1 Application Purview

Area	Description	Mandatory [Y/N]
1. Implementation Plan	Feedback from previous test implementations completed.	Y
2. System Support Document(SSD)	Ensure SSD completed and accurate.	Y
3. Technical Documentation	Appropriate documentation has been produced for use by staff providing technical support for the new enhanced application.	Y
4. Scalability/Load Testing	Adequate load testing has taken place and results recorded.	N
5. Performance	The application has been tested against stated performance criteria. Performance has been assured by user and support staff testing.	Y
6. Configuration Management Database	The relevant details regarding new or changed infrastructure components have been added to the configuration management database.	Y
7. Change Control	A change control entry has been created for the LIVE implementation.	Y
8. Test Log Review	A review of the test log has taken place to ensure all required actions have been completed.	Y
9. Production Management Handover	Handover to Production Management is completed and the team are in are in position to support the application post deployment.	Y
10. Environment comparison	Database comparison between legacy and target system.	N
11. Client requirements	Does the application have specific client requirements, such as JVM/JRE versions, JInitiator? If so have these requirements been raised with Desktop services	Y
12. Technologies	Is there any new software or technologies involved?	N

Table 2 Infrastructure Purview

Area	Description	Mandatory [Y/N]
1. Technical Architecture Document(TAD)	Mapping of legacy system architecture and target system architecture completed.	Y
2. Security	All security requirements, e.g. SSL encryption, IP based restrictions firewall requirements have been specified, tested and implemented.	Y
3. Patching	Ensure any new or amended infrastructure is included in regular evolving process. Different technologies may follow different strategies and ensure the new infrastructure is added to any existing processes and documents.	Y
4. Asset Register	Details of any new hardware acquired as part of the project have been recorded.	Y
5. Infrastructure view	All infrastructure diagrams are updated with newest server and infrastructure details.	Y
6. Start/Stop scripts	Are Server Start-up/Shutdown scripts in place? Including start up procedure documented	Y

Table 3 Support Purview

Area	Description	Mandatory [Y/N]
1. Support Agreement (including any charging arrangements)	A support agreement is in place for any new applications – including any hosting or support charges.	Y
2. System Description Document	Documentation complete and reviewed by support group	Y
3. Time Recording Code	A Time Recording code for the application, if required, has been confirmed and set up.	Y
4. Backup and Recovery	All backups need to be confirmed operational.	Y
5. Test Environment	An adequate test environment has been established for the application which may be used by support to test future changes prior to implanting these in the live environment.	Y
6. Hardware and Software Licensing	All required licensing is in place including maintenance/support arrangements with external suppliers.	Y
7. Help Desk	The new application is recognized with the helpdesk.	Y
8. User Guide Documentation	Appropriate documentation has been produced for users of the new application.	Y
9. Training Material	Training material, if required, has been produced and is of an appropriate standard.	N
10. Demonstration or Walkthrough	Demonstration or walkthrough of the new application has taken place for other stakeholder.	N
11. Deployment Date	Agreed date has been confirmed that allows adequate time for completion of Acceptance Sign Off Review.	Y
12. Deployment Resources	Resources required for deployment, including those needed for post implementation checking and sign off have been secured.	Y
13. Service Announcement	A Service announcement has been raised with the agreed deployment date on the alert system	Y

Table 4 Score Board

S. No.	Purview	Score Value (Y-1,N-0)	Remark
1	Application purview		
2	Infrastructure purview		
3	Support purview		
	Total Value		

- *Organizational risk component*

The organizational risk measurement model measure organizational structure, attitudes, experience as well as objectives and values (personal and cultural) of the organization in which legacy system operates to support system evolution through reengineering. Following factors affect impact value of organizational risk component.

1. Quantitative overload, qualitative overload

If Individuals are in a quantitative work overload situation and working under pressure and have too much work to do in too short time it will cause lack of interest for evolution decision of legacy system. This form of overload has been a major reason for the failure of reengineering effort [16].

2. Role conflict and ambiguity

Organizational policy of giving repetitive and monotonous jobs generates role conflicts and ambiguity thus decrease motivation and satisfaction at work, thus increasing absenteeism rates to contribute in reengineering effort.

Role conflict occurs when individuals are faced with incompatible or contradictory expectations by their superiors or co-workers, or even when these expectations contradict the employees' values, beliefs or goals.

Role ambiguity occurs when individuals do not know what is expected of them, what tasks to perform, or what their responsibilities are in the context of their work.

3. Participation in decision making process

The degree to which individuals participate in the organization's decision-making process is an important element for the effectiveness of the organization. Greater involvement of workers in the decision-making process gives them the opportunity to improve communication and fosters social support within the organization.

4. Physical environment and working conditions

An unhealthy physical environment and difficult working conditions also increases impact value of organizational risk component. These factors can have negative effects on the level of performance, satisfaction and motivation at work.

5. Work schedules

Excessive work schedules can also contribute to increase impact of organizational risk component. Excessive hours of work do not necessarily increase productivity but tend to decrease individuals' effectiveness and efficiency.

6. Recognition

Lack of recognition policy at work linked to motivation and satisfaction at work and will affect organizational risk component.

7. Interpersonal relations

The quality of the relations between individuals in the context of their work can have an impact on organizational risk component. There are generally three levels of interpersonal relations in an organization: relations with peers or co-workers, with management and with clients.

8. Information Flow

Open and transparent communication should be encouraged within the organization to reduce impact level of organizational risk component.

Table 5 Impact Calculation of Organizational Risk

S. No.	Measure	Scale value 1. Poor-0 2. Average-1 3. Satsfactory-2 4. Good-3
1	Quantitative overload, qualitative overload	
2	Role conflict and ambiguity	
3	Participation in decision making process	
4	Physical environment and working conditions	
5	Work schedules	
6	Recognition	
7	Interpersonal relations	
8	Information Flow	
	Total	

Table 6 represents important measures and scale value used to compute Total impact of organizational risk component.

Once we have identified the key measures a measurement metrics is developed to compute total impact of organizational risk component (TIOR).Impact of each measure can be calculated by using a scale value that represents to what extent users of legacy system and developers of target system agree or disagree for respective measure. If we use a scale of 0 (poor) to 3 (good) 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.

$$(\mathrm{TIOR}) = \sum_{i=1}^{n} (X)$$

Where

X represents scale value given by legacy system users and developers of target system

I represent number of measures

- *Resource Risk component*

Resource risk measurement model measures availability and quality of resources that includes hardware, software human and reusable components in accordance with the available budget, schedule and strategic objectives of reengineering to evolve legacy system. Resource availability for system evolution determines the periods during which a selected resource is required for a specified duration, starting from a specified time. The duration can be continuous or it can be divided into separate segments, depending on the requirements of system evolution task [17]. The total impact of resource risk (TIRR) is measured using following metrics

TIRR = AWH+ AC

Where

AWH represents Annual Working Hours

AC represents Annual per Time Unit Cost

Measures of resource Risk

1. Number of Resources (No.) = Number of required resources available for the system evolution task
2. Average Cost per time unit of required resources AVERAGE (Cost per Time Unit)
3. Total Duration (The combined duration of all time slots when a particular resource is required) SUM (Duration of all resources)

Where Total Duration

Start Time = the start time of the period of resource requirement

End time = the end time of the period of resource requirement

Duration = the duration of the period of resource requirement (End Time - Start Time)

Total duration=the combined duration of all periods when the resource is required

SUM (Duration)

1. Total Cost per Time Unit (The total costs incurred for costs per time unit for the entire period)
   SUM (Total per Time Unit Cost)

2. Annual Working Hours (The annualized number of hours that at least one required resource is available)
   AWH= (Total Duration in hours) * (No. of resources) / (period of Evolution in hours)

3. Annual per Time Unit Cost (The annualized cost of the resource)
   AC = (Total Cost per Time Unit) * (No. of resources) / (period of Evolution in hours)

- *Development process risk*

Development process risk measurement model measures different components of development process in order to achieve acceptable decision towards reengineering option. Identification of development process risk requires objectives of organization by bringing together human, physical and financial resources in an optimum combination and making the best decision for the organization while considering reengineering option for the evaluation of legacy system. The total impact of development process risk (TIDPR) component can be computed using following metrics

$$(\text{TIDPR}) = \sum_{k=0}^{n} (\text{DRE})$$

Where

DRE represents Defect Removal Efficiency

K represents no. of phases

Defect Removal Effectiveness is an important metrics to measure development process risk component

Defect removal effectiveness can be defined as follows

$$\text{DRE} = \frac{\text{Defects removed during a development phase} * 100\%}{\text{Defects latent in the product}}$$

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 estimated by

Defects latent in the product = Defects removed during the phase + defects found later

The metrics can be calculated for the entire development process, for the front end, and for each phase. It is called early defect removal and phase effectiveness when used for front end and for specific phases, respectively. The higher the value of the metric, the more effective the development process and a few defects escaped to the next phase or to the field [18].

Process metrics aim at given the management team and the development team the following:

• An accurate assessment of progress to date

• Insight into the quality of the evolving software products

• A basis for estimating the cost and schedule for completing the product with increasing accuracy over time

- *Personal risk component*

Personal risk measurement model identify and measures comfort ability of personals both users of legacy system and developers of target system with the system evolution objectives through reengineering. It involves job matching, team building, moral building, schedule and financial aspects of system evolution at personal and organizational level [19].

1. Job Matching- Type of job assigns and job interest of developer for target system.
2. Team building- Type of team organization and characteristic of a person involves in the evolution process of legacy system.
3. Moral building –Moral level of all stakeholders involve in the evolution process of legacy system.
4. Schedule aspects- level of Uncomfortability between evolution schedule and availability of users of legacy system and developers of target system.
5. Communication Skill- Ability and skill level of interaction with users of legacy system and developers of target system.
6. Financial aspects – organizational financial policy and rules that will affect satisfaction level of users of legacy system and developers of target system in the evolution process.

Table 6 Impact Calculation of Personal Risk

S. No.	Measure	Scale value 1. Poor-0 2. Average-1 3. Satsfactory-2 4. Good-3
1	Job Matching	
2	Team building	
3	Moral building	
4	Schedule aspects	
5	Communication Skill	
6	Financial aspects	
	Total	

Once we have identified the key measures a measurement metrics is developed to compute total impact of personal risk component (TIPR) shown in table 7 .Impact of each measure can be calculated by using a scale value that represents to what extent users of legacy system and developers of target system agree or disagree for respective measure. If we use a scale of 0 (poor) to 3 (good) 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 total impact of personal risk component (TIPR) can be computed using following metrics

$$(\text{TIPR}) = \sum_{i=1}^{n} (X)$$

Where

X represents scale value given by legacy system users and developers of target system

I represent number of measures

V. EXPERIMENT AND ANALYSIS

The objective of this experiment is to check the precision of the mentioned quantitative risk measurement model for infrastructure perspective of legacy system and compare the result of two legacy software of the same scenarios i.e. library management system. The two different legacy library management systems are used to check the correctness of proposed measurement model. The total impact of five identified risk is calculated for each legacy library management system using different measurement metrics for respective risk components.

Applying pentagram model to five risk components we have the following results as shown in table 8.

TRI (LS1) = 0.48 X (ab+bc+cd+de+ea)

TRI (LS1) =0.48 X [(.30*.20) + (.20*.25) + (.25*.40) + (.40*.40) + (.40*.30)]

TRI (LS1) = .235

TRI (LS2) = 0.48 X (ab+bc+cd+de+ea)

TRI (LS2) =0.48 X [(.40*.30) + (.30*.35) + (.35*.50) + (.50*.50) + (.50*.40)]

TRI (LS2) = .408

Where LS1 represents legacy system 1

LS2 represents legacy system 2

TRI Total Risk Impact

Table 8 Result

System	a	b	c	d	e	TRI
LS1	.30	.20	.25	.40	.40	.235
LS2	.40	.30	.35	.50	.50	.408

Based on the TRI values of two legacy library management system the measurement results for both systems i.e. LS1 and Ls2 tests are shown in Figure 2. It is clear that the TRI of LS2 (Right) is higher than the TRI of LS1 (Left).

A mean opinion score represented in table 9 is used to quantify and predict the judgment based on total impact of reengineering risk from infrastructure perspective of legacy system.

Table 9 Mean Opinion Score

Level of Satisfaction	Risk Impact	Range of values
Reengineering Successful	Low TRI value	0-1
Need Risk Resolution Strategy	Average TRI value	1-1.5
Massive Risk Engineering /Reengineering Failure	High TRI values	1.5-2.4

We give comparative TRI values for LS1 and LS2 with the mean opinion score. The mean opinion scores and the corresponding measurement model based impact values are shown on the table 9. It shows that reengineering is successful if the TRI value is less than or equals to 1 and the values higher than this level required massive risk engineering or tends to reengineering failure.

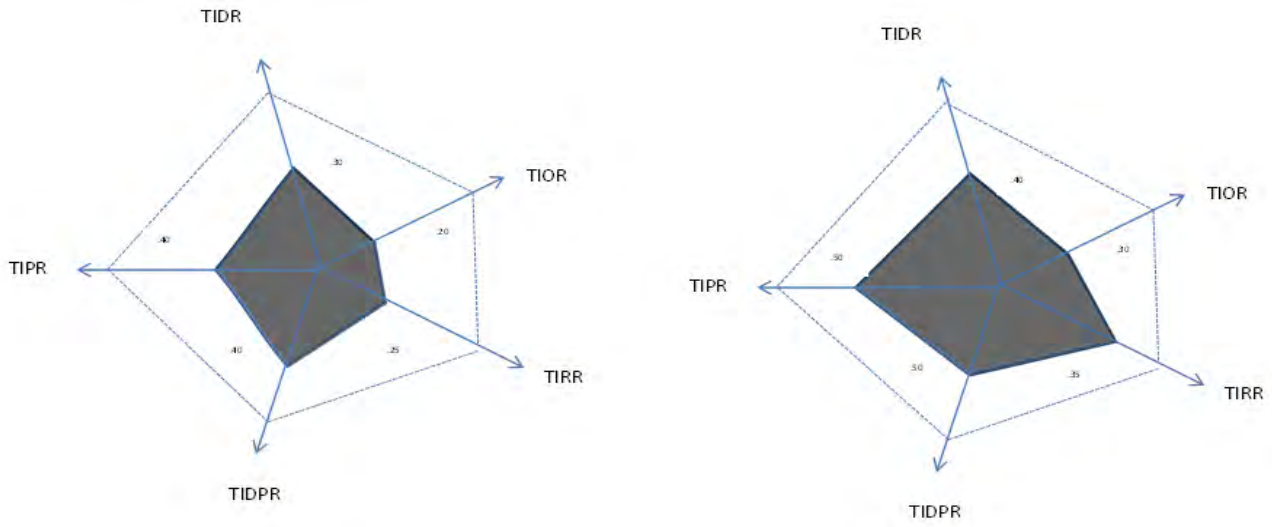

Figure 2 Comparative analysis

VI. CONCLUSION

Renovation of legacy system is a very important factor for the success of any software organizations. They have to change their legacy system with respect to product, processes and services in order to keep high competitiveness in the market. Software reengineering is a modernizing technique used to modify structure and values of the legacy system systems data and services.

Successful legacy system reengineering requires effective measurement of reengineering risk to facilitate developers and client of the legacy system to be aware and measure total impact of all the risk that could be identified in system, managerial and technical domains of legacy system. We present a quantifiable measurement model to estimate comprehensive impact of different reengineering risk arises from infrastructure perspective of legacy system. The model consists of five reengineering risk component, including Deployment Risk, Organizational Risk, Resource Risk, Development Process Risk and Personal Risk component. Proposed risk measurement model and mean opinion score board offers better performance in terms of risk measurement to support the decision-making process.

REFERENCES

[1] Brodie, M.L., Stonebraker, M.: Migrating Legacy Systems: Gateways, Interfaces, & theIncremental Approach. Morgan Kaufmann Publishers, Inc., San Francisco (1995)

[2] Sommerville, I.: Software Engineering, 7th edn. Pearson Education, London (2006)

[3] The management of software engineering, Part I: Principles of software engineering. IBM Systems Journal 19(4), 414–420, ISSN: 0018-8670, doi: 10.1147/sj.194.041

[4] Anand Rajavat, Vrinda Tokekar, "ReeRisk –A Decisional Risk Engineering Framework for Legacy System Rejuvenation through Reengineering", Published in Proceedings of Second International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2011 by Springer LNCS-CCIS, March 10-11, 2011 in Bengaluru, India, CNC 2011, CCIS 142, pp. 152 – 158, 2011, © Springer-Verlag Berlin Heidelberg 2011.

[5] Ransom J., Somerville I., Warren I. ," A Method for Assessing legacy systems for evolution," in Proceedings of the Second Euromicro Conference on Software Maintenance and Reengineering, 1998,ISBN: 0-8186-8421-6, Digital Object Identifier : 10.1109/CSMR.1998.665778

[6] Byrne, E.J. Gustafson, D.A.," A software re-engineering process model", in Proceeding of, Sixteenth Annual International Conference on Computer Software and Applications, Digital

Object Identifier: 10.1109/CMPSAC.1992.217608 , ISBN: 0-8186-3000-0 ,1992 , PP 25-30.

[7] Er.Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "Identification and Measurement of Functional Risk Components in Reengineering Process of Legacy System", Published in International Journal of Advanced Software Engineering (IJASE), ISSN 2249-3069 Volume 1, Number 1 (2011), © Research India Publications ,pp. 11-25.

[8] Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "RrMm- a Measurement Model to Quantify the Effect of Reengineering Risk in Quality Perspective of Legacy System" Published in Springer International Conference on Advances in Information Technology and Mobile Communication – AIM 2012,PP 9-16 © Springer-Verlag Berlin Heidelberg 2012.

[9] Pontus Svensson, Dzagen Milicic ," Sparks to a living quality Organization- A total quality approach towards improvements", A master thesis in software engineering, Department of Computer Science and Business Administration, University/College of Karlskrona/Ronneby, 1998.

[10] P k Suri, Manoj Wadhwa,"Identification and assessment of Software Project's Risk ", international Journal of computer science and network security,VOL.7 No.8 August 2007.

[11] Trivedi, K.S.; Vaidyanathan, K.; Goseva-Popstojanova, K," Modeling and analysis of software aging and rejuvenation", Proceedings. 33rd Annual Simulation Symposium, 2000, Digital Object Identifier: 10.1109/SIMSYM.2000.844925, 2000, pp270-279.

[12] Paul R. Garvey, Chien-Ching Cho,"An Index to measure a system's performance Risk, Technical report, Report Number: A725324, Report Date: 2003, pages 13.

[13] Paul R. Garvey, Chien-Ching Cho,"An Index to measure a system's performance Risk, Technical report, Report Number: A725324, Report Date: 2003, pages 13.

[14] Er.Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "An Impact-based Analysis of Software Reengineering Risk in Quality Perspective of legacy System", Published in International Journal of Computer Applications (IJCA), November 29, 2011, ISBN: 978-93-80865-35-6, Doi 10.5120/4046-5794, PP: 40-47.

[15] Er.Anand Rajavat, Dr. (Mrs.) Vrinda Tokekar, "Quantitative Evaluation Of Managerial Risk Components In Reengineering Process Of Legacy System", Published in International Journal of Software Engineering (IJSE) International Research Publication , ISSN 0974-3162, Volume 3, Number 1 (2012), pp. 35-47

[16] Janne Ropponen and Kalle Lyytinen," Components of Software Development Risk: How to Address Them? A Project Manager Survey," IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 26, NO. 2, FEBRUARY 2000

[17] Aditya Agrawal, Dr. Gavin Finnie, Dr. Padmanabhan Krishnan," ORE: A Framework to Measure Organizational Risk During Information Systems Evolution," Technical Report CSA07-02, Centre for Software Assurance Faculty of Information Technology Bond University Gold Coast, Queensland Australia

[18] "Risk Assessment Template for Software Development or Acquisition Projects" Technical report, Niwot Ridge Consulting, Niwot, Colorado.

[19] Dr. Thomas Fehlmann," Metrics for Cooperative Development Processes", Euro Project Office AG, Zurich, Switzerland, IWSM/MetriKon 2004.

[20] Personnel risk management, Toolkit, supported by European agency for safety and health at work.