SysRisk –A Decisional Framework to Measure System Dimensions of Legacy Application for Rejuvenation through Reengineering

Er. Anand Rajavat
Computer Science & Engineering
Shri Vaishnav Institute of Technology And Science
Indore, M. P., India

Dr. (Mrs.) Vrinda Tokekar
Information Technology
Institute Of Engineering and Technology(DAVV)
Indore, M. P., India

ABSTRACT
Software reengineering is the concept of gracefully modernizing a legacy application. Many organizations are planning to modernize their legacy application through reengineering .However many of these efforts are often less than successful because they concentrate on a narrow set of risk issues without fully considering a broader set of enterprise wise system, managerial and technical risk issues. Overall success of reengineering effort requires a decision driven risk assessment framework that examines system, managerial and technical domain of legacy application. We present a hierarchical system domain risk framework SysRisk to analyze system dimensions of legacy application. The fundamental premise of framework is to observe, extract and categories the contextual perspective models and risk clusters of system domain. This work contributes for a decision driven framework to identify and assess risk components of system domain. Proposed framework provides guidance on interpreting the results obtained from assessment to take decision about when evolution of a legacy system through reengineering is successful.

General Terms
Reengineering, Risk engineering, legacy System

Keywords
SysRisk, Domain, Perspective.

1. INTRODUCTION
Organization which has been using information technology for more than five years has a legacy software problem. Most of the legacy system [1] 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. However organizations must consider modernizing these legacy systems to remain viable. Over the past few years, legacy system reengineering has emerged as a popular modernization technique. Reengineering [2] offers an approach to migrate a legacy system towards an evolvable system in a disciplined manner. The process of reengineering may be viewed as applying reengineering principles to an existing system in order for it to meet new requirements. Software reengineering projects is often faced with unanticipated problems which pose risks within the reengineering process. Successful Implementation of reengineering effort requires an understanding of the current and desired system state and available reengineering technology by identifying and controlling risk from system, managerial, and technical domain of legacy application.

System domain denotes a structural unit that is responsible for maintaining a system that provides products and services to its customers. In this context, the System is responsible for planning and structuring the system Infrastructure efforts, organizing the stakeholder's tasks and ensures that the products and services fulfill the organization's goals and objectives.

Managerial domain covers managerial issues related to system evolution process .Impact of market factors and effect of competitive products, on quality [3] & cost of target system are measured within the context of managerial domain. Managerial domain identifies and measure organizational economic value to support system evolution activities.

Technical domain has a significant impact on software functionality and software quality. Technical domain helps in analyzing and testing the legacy system to better understand the function's capabilities and quality features and assess the impact of the proposed changes.

Present work describes the initial establishment of a system domain risk framework SysRisk to identify and measure risk components of system domain in accordance with requirements of target system. SysRisk framework identifies and analyze risk arise from organizations and stakeholders point of view. Proposed system domain risk framework SysRisk is intended to help identify and measuring effect of system domain risk triggered by actual measurements in reengineering process of software system. The SysRisk framework is applied to an in-use legacy system to identify and categories risk components of system domain and to measure cumulative effect of different risk components. Finally, this paper contributes to analyze the cause-effect relationship between the reengineering process and existing state of legacy system in accordance with target system requirements.

2. RELATED WORKS
In recent years, considerable attention has been devoted to the phenomenon of software reengineering [4] [5]. In the past years, research work in the area of reengineering focuses on the development of different reengineering frameworks, but very few research works identify risk factors in reengineering process of software systems. Reengineering risk and their influence on software quality causes reengineering efforts to fail. For the development of successful reengineering effort reengineering risks need to be managed.

Peter H. Feiler in [6] discusses a plan, for reengineering to improve the cost-effective evolution of large software-intensive systems .The focus of this paper is on technical

aspects of reengineering. However, economic, management, and quality aspects of a system play an important role in the successful implementation of reengineering efforts.

Harry M. Sneed in [7] summarizes the results of 13 reengineering projects conducted during the past 10 years. Analyses show that software reengineering projects have a significantly lower risk factor than software development projects – 25 % as opposed to 57 %. This difference can be calculated in terms of project completion rates and cost overruns. However selection of reengineering effort also required considering other factors like performance improvement, resource utilization, quality goals, user satisfaction etc.

Eric K. Clemons Michael C. Row Matt E. Thatcher in [8] suggests that two principal reasons for failure of reengineering efforts are functionality risk and political risk, respectively. Though there is other serious risk such that technical risk, process risk, development environment risk, architecture risk, and risk related to stakeholders are also causes the reengineering efforts to fail.

Software reengineering disasters indicate that their problems would have been avoided or strongly reduced if there had been an explicit early concern with identifying and resolving their high-risk elements. Proposed SysRisk framework analyzes various risk components of system domain and expresses cumulative effect of risk due to various risk components. The system domain risk framework SysRisk is intended to help identify and measuring effect of system domain risk triggered by actual measurements in reengineering process of software system.

3. SysRisk (SYSTEM DOMAIN RISK FRAMEWORK)

The term "System domain" denotes a structural unit that is responsible for maintaining a system that provides products and services to its customers. In this context, the System is responsible for planning and structuring the system Infrastructure efforts, organizing the stakeholder's tasks and ensures that the products and services fulfill the organization's goals and objectives. The element of the System domain risk framework SysRisk consists of Infrastructure perspective model and Stakeholder perspective model.

The system domain addresses the requirements of the customer, the organization's strategic goals and objectives and the operational environment of the enterprise. The system domain concentrates on the current legacy systems and their operational environment as well as how the proposed system will be affected by (or affect) elements of system domain.

The system domain risk framework covers two different perspectives of software development process [9] that are essential for developing and implementing system domain risk framework. For each perspective one or more risk clusters are identified which includes risk component and the risk measurement model. Critical risk factors for each risk component are identified to support measurement model, which is used to measure the effect of particular risk component.

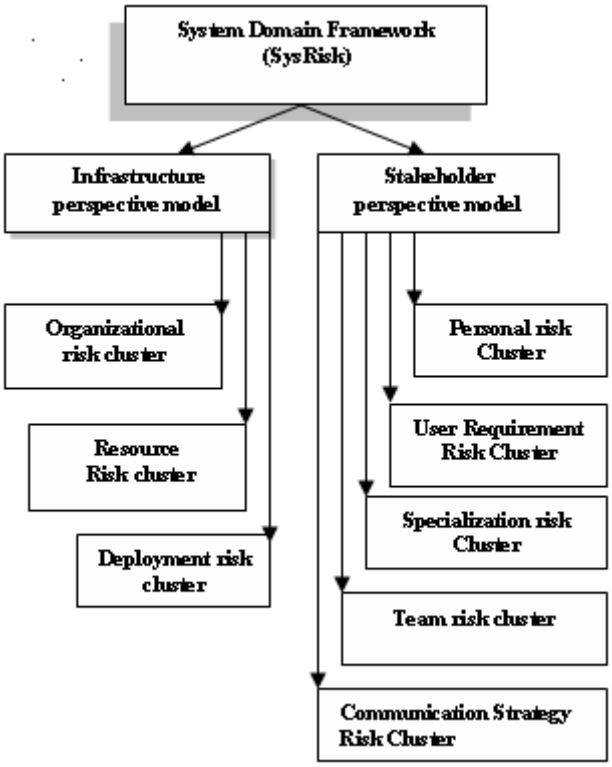

Fig1: System domain risk framework SysRisk

A simplified conceptual view of the elements in system domain risk framework SysRisk is presented in Figure -1, framework comprises with Perspective, risk cluster and risk factors.

Perspective is a viewpoint according to which different risk clusters are identified and measured using different risk measurement model.

Risk cluster covers risk component and the risk measurement model, which is used to measure the effect of particular risk component on system evolution decision.

Risk component contain different types of negative outcomes from system domain of legacy application.

Risk measurement model measures different types of risk components from system, managerial and technical domain of legacy system in accordance with desired state of target system and reengineering strategy.

Risk factor encompasses sources of risk components from system domain of legacy application.

System domain is characterized in terms of a fundamental set of risk component and factors that are indicative of the present state of legacy and desired state of Target System. In SysRisk framework two types of perspective model i.e. Infrastructure perspective Model and Stakeholder Perspective Model is developed by analyzing states of legacy and Target system.

3.1 Infrastructure Perspective Model

Infrastructure Perspective Model is a function of the particular organization, its available resources, its project structure and its practices. Model describe state of organization by analyzing infrastructure support they provide, the process they used and the work product they produces to support target

system requirements. Risk clusters for infrastructure perspective model are:-

3.1.1 Organizational risk cluster

Organizational risk component: - Organizational risk component is the risk of loss resulting from inadequate or failed internal organizational structure, undefined objectives and values, complex processes and uncertainty in the organization's activities.

Organizational risk measurement model: - 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.

Organizational objectives can be defined as the specific collection of values and norms that are shared by people and groups in an organization and that control the way they interact with each other and with stakeholder outside the organization.

3.1.2 Resource risk cluster

Resource risk cluster comprises with resource risk component and measurement model.

Resource risk component:-Resource risk component is the risk of loss associated with unavailability or delay and low quality resources to support system evolution activity.

Resource risk measurement model: - Resource risk measurement model measure the 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.

3.1.3 Deployment risk cluster

Deployment risk cluster comprises with deployment risk component and measurement 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:-Deployment risk measurement model measures the present organizational structure with the view of target system deployment. Identification and measurement of deployment risk require to considering organizational operational environment, organizational structure, network capability, hardware, and software support and user skill level.

3.2 Stakeholder Perspective Model

Stakeholder perspective model expresses roles and responsibility of stakeholders for a particular organization. Model covers user and developer's thinking towards reengineering option for the evolution of legacy system. Issues like team organization, communication strategy, personal comfort ability and skill set are also addressed in the context of stakeholder perspective model. Risk Clusters for Stakeholder Perspective Model are:-

3.2.1 Personal risk cluster

Personal risk cluster comprises with personal risk component and measurement model.

Personal risk component:-Personal risk component is the risks of loss associated with uncomfortability of personal (user and developer) with the system evolution objectives.

Personal risk measurement model: - Personal risk measurement model identify and measures comfort ability of personals both user and developer 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.

3.2.2 User requirement risk cluster

User requirement risk cluster comprises with user requirement risk component and measurement model.

User requirement risk component: - User requirement risk component is the risk of loss associated with present state of legacy system to support implementation and deployment of desired requirements of the target system.

User requirement risk measurement model: - User requirement risk measurement model measures requirements of the target system as expressed by the users by considering the present state of the legacy system. Identification of user requirement risk involves defining customer needs, goals and objectives of target system in the context of the organizations operational environment.

3.2.3 Specialization risk cluster

Specialization risk cluster comprises with specialization risk component and measurement model.

Specialization risk component:-Specialization risk component is the risk of loss associated with inexperience and amateur workforce for system evolution.

Specialization risk measurement model:-Specialization risk measurement model measures the overall technical and development expertise and experience of the software engineering that will be involve in reengineering process. Identification and measurement of specialization risk requires considering 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 that will use to achieve goals of desired target system.

3.2.4 Team risk cluster

Team risk cluster comprises with team risk component and measurement model.

Team risk component:-Team risk component is the risk of loss associated with complex team organization and complicated team oriented activities.

Team risk measurement model: - Team risk measurement model measures team-oriented activities of customer and developer. Identification of team risk requires considering shared product vision, target results, and objectives of organization. Team risk identify and measure the attributes of organizational structure and operational activities for the evolution of legacy system throughout the all phases of the reengineering life-cycle such that all individuals within the organizations, groups, departments, and agencies directly involved in reengineering are participating team members.

3.2.5 Communication strategy risk cluster

Communication strategy risk component:-Communication strategy risk component is the risk of loss associated with communication gap and communication conflicts between stakeholders.

Communication strategy risk measurement model: - Communication strategy risk measurement model measures, process for exchange of information and opinion of individuals, groups, and organization on communication process. Identification of communication strategy risk consider medium and approach of communication as well as identify different factors for communication gap between stakeholders. Risk highlights more clearly the nature and size

of the communication conflict. Identification and resolution of communication risk is implicit in the reengineering action since it requires effective and proper communication between stakeholders of legacy and target system.

4. CONCLUSIONS

The reengineered system replaced the legacy one to the satisfaction of all the stakeholders; the reengineering process also had a satisfactory impact on the quality of the system. Proposed framework SysRisk analyzes various risk components of system domain and expresses cumulative effect of risk due to various risk components. In this paper, we first categorize major perspective models and risk clusters of system domain for legacy application to identify and analyze various risk components .We then construct a system domain risk framework SysRisk to establish correlation between various perspective models and risk clusters. This work contributes for a goal driven risk engineering framework to identify and assess risk within the system domain of legacy system. The paper proposes a system domain risk framework SysRisk, which is applied to an in-use legacy system to identify and categories risk components of system domain and to measure cumulative effect of different risk components. The SysRisk framework guides users through assessment of system domain by selecting assessment measures and assigning values to them. The result of SysRisk framework is a level of understanding to take decision about when evolution of a legacy system through reengineering is likely to succeed and when they are likely to fail.

5. REFERENCES

[1] Brodie, M. L., Stonebraker, M., "Migrating Legacy Systems: Gateways, Interfaces, & the Incremental Approach," Morgan Kaufmann Publishers, Inc.; 1995.

[2] 665778 searchabstractRansom 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

[3] Boehm, Barry , Chulani, Sunita , Verner, June , Wong, Bernard," Fifth Workshop on Software Quality", in 29th International Conference ICSE 2007 Companion on Software Engineering - Companion, 2007, ISBN: 0-7695-2892-9 , Digital Object Identifier : 10.1109/ICSECOMPANION.2007.38 , PP. 131 – 132.

[4] Paul Briden, "Software Re-engineering process," Tessella Support Services PLC Technical report, Issue V2.R1.M1, 2000.

[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 , INSPEC Accession Number: 5884288,PP 128 – 134.

[6] Peter H. Feiler, "Reengineering: An Engineering Problem," Technical Report Software Engineering Institute Carnegie Mellon university Pittsburgh Pennsylvania 15213, CMU/SEI-93-SR-5, 1993.

[7] Harry M. Sneed, "Risks Involved in Reengineering Projects," in WCRE: Proceedings of the Sixth Working Conference on Reverse Engineering-1999, IEEE Computer Society pp.204.

[8] Eric K. Clemons Michael C. Row Matt E. Thatcher, "An Integrative Framework for Identifying and Managing Risks Associated With Large Scale Reengineering Efforts," in 1995, Proceedings of the 28th Annual Hawaii International Conference on System Sciences - 1995 pp. 960-969.

[9] Russ, M.L. , McGregor, J.D. , Korson-McGregor, Clemson, SC ,"A software development process for small projects", in Software IEEE , ISSN : 0740-7459 , Digital Object Identifier : 10.1109/52.877874, PP 96 – 101.