Information Management and Business Review
Vol. 4, No. 2, pp. 79-85, Feb 2012 (ISSN 2220-3796)

Six Sigma based Risk Identification and Mitigation Framework for Projects Execution

*Muhammad Usman Tariq, Muhammad Naeem Ahmed Khan
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan.
*usman_kazi2006@yahoo.com

Abstract: Six Sigma being a project management methodology is used in the industries and corporate sectors to substantiate goal of near perfection in process implementation and execution. It is based on the impetus of Plan-Do-Check-Act and has myriads of applications in numerous organizational and business processes to attain significant performance improvement in different industrial and corporate sectors including the IT sector. Despite realization of profuse maturity in many business processes, Six Sigma still lacks across-the-board framework for effective risk management because root cause analysis (RCA) is still the primary and principal technique used for handling risks in this methodology. In this paper, we have attempted to put forward a risk identification framework in order to improve quality and productivity of Six Sigma projects, particularly the IT development projects. The study also encompasses an abridged overview of the current methods being practiced for risk identification in Six Sigma. Our proposed model enlist a number of hypotheses for validation purposes and is duly evaluated and analyzed viz-à-viz DMAIC and DMADV approaches to make it compatible with QFD, FMEA and PMBOK requirements.

Keywords: *Risk management in Six Sigma, Quality Management, Process Capability, Process Analysis, Risk Assessment Models, and Project Management.*

1. Introduction

Six Sigma is a set of best practices for enhancing manufacturing processes and reducing production defects and is often termed as problem solving methodology that involves statistical techniques (De-Feo & William, 2005). Over the time, Six Sigma expanded its horizon to address numerous organizational and business processes. Six Sigma received standing recognition in different domains for process improvement including software processes. Six Sigma ordinarily consists of two approaches: - define-measure-analyze-improve-control (DMAIC) and define-measure-analyze-design-verify **(**DMADV) also called Design for Six Sigma (DFSS). Six Sigma is based on DMAIC philosophy and focuses on finding root cause of the problem using statistical methods. Risk can be defined as an unexpected occurrence of an event that could have a positive or negative effect on the development and execution of the project. Six Sigma offers specialized tools and techniques for process improvement; however, it lacks risk-handling processes apart from RCA. Risk identification and handling is always a major concern of the industry in real time environment and this aspect lead as a prime motivation for us to undertake this study. Risk analysis deals with analyzing the possible risks and their effects to minimize the risk effects; hence, risk must be identified and managed to minimize the probability of occurrence (Alhawari et al., 2008) in order to make a project successful.

Software development projects are particularly difficult as most of the new products require prior research and may carry a high risk factor. Even though, a number of risks can be identified beforehand, but the probability of failure remains greater. In this paper, we have attempted to propose risk identification and mitigation framework based on Six Sigma philosophy for potential use in different corporate sectors particularly the IT sector. The study also takes account of different risk management frameworks that can be effectively utilized to improve productivity. The framework is designed with particular reference to improving quality and productivity of the Six Sigma projects. For this purposes, various Six Sigma techniques have been explored as part of the literature survey to highlight how they can be employed and exploited by the organizations and businesses to enhance their overall processes in order to succeed through all the development stages of a project. Scope creep – a common phenomenon with software projects, also critically affects software projects being language and system dependent. The frequent changes and complexity of the project also compromise its quality; therefore, a proper risk management is required for IT projects (Deng

and Ma, 2008). Risk identification and mitigation process collectively known as risk management is an important part of any project. In Six Sigma, it is employed as a critical phase called RCA. It has been widely used for transforming the effects of risks and minimizing them to greater extent.
The core approach used in RCA is to identify origins and reasons of the problems within different processes that introduce defects in the product. A priority table is usually used to identify the critical risk and classify them according to their level of severity and impact. A number of tools are applied in Six Sigma measurement analysis phase to identify, prioritize and classify the processes. In project management, risk identification is an intrinsic phase, whereas in Six Sigma, it is embedded into every phase. Due to the dissimilarity of risk management approach, this research is intends to aptly implement risk management into every phase of the project using Six Sigma tools. Presently, no Six Sigma based risk management framework is being used in the industry. The implementation of our proposed framework could lead to risk identification and defect removal from a project concurrently as well as minimize the time factor for carrying out these activities. This section presents an overview of Six Sigma methodology with particular reference to risk identification and mitigation strategies. The next section provides an overview as well as critical analysis of the existing Six Sigma tools and techniques. The theoretical framework is outlined in the third section and the list of hypotheses developed to test the validity of the model is summarized in the fourth section. Fifth section describes our proposed framework for risk identification. Some future dimensions to this research are sketched out in the sixth section and finally we conclude in the last section.

2. Literature Review

Risk has always been an issue in projects execution and many projects fail due to uncertain and unexpected risks that emerge during the project execution. Indeterminate events are embedded within the risks associated to a project and they typically float up unexpectedly. FMEA (Failure Mode and Effect Analysis) is part of DMAIC and DMADV and is used for identifying possible failure risks in project processes. A comparison among the important concepts related to risk management tools and techniques particularly FEMA and PMBOK (Project Management Body of Knowledge) have been drawn in Santos and Cabral (2008); and FMEA is combined with PMBOK to utilize both the techniques to create a new model for identification of risk. Cost overrun in IT projects is quite common and proper implementation of risk management is required to make project a success. Six Sigma is mostly defined in terms of defect rate metric, tool and improvement program (Park et al., 2007). It needs to be acknowledged that Six Sigma is an industrial implementation and hardly any industry shares the knowledge due to its policies and cost incurred on implementing Six Sigma methodology. The need for conducting wide-ranging research on Six Sigma has been stressed in (Zhang et al., 2009) as Six Sigma minimizes the product defects to a very low level.

The theme of the Six Sigma is to focus on customer wants and factual decisions based on process improvement, organizing data, contemplating stakeholder linked to the specific project and retaining a space for experimentation. All these characteristics when combined together give perfection for Six Sigma. Wang (2008) discusses issues related to subcategory of Six Sigma like DMIAC, DFSS and deployment. Six Sigma involves many tools such as control charts, fishbone and failure mode analysis that help to analyze the data and find out the actual cause of the defect. Wang et al. (2010) report that applying QFD technique on a project not only increases efficiency, but also reduces cost and time. A lesser amount of research is carried out in the area of enterprise level risk management. Earlier, some frameworks were developed such as ARMF (Alternative Risk Management Framework) but it covers only three components: theoretical risk management, applied risk management and model implementation. Azizi and Hashim (2008) present a risk assessment framework at industrial level, which highlights that calculations involved in businesses are based on tools, software and network.

Likewise, root cause of generation of risk primarily depends on the machines, which are never error free. Success of a project is primarily based on managing risks that intermittently occur during the execution of projects. In this perspective, the basic model presented by PMBOK helps to identify, evaluate, monitor and control the risk (Rovai et al., 2006). Any model based on PMBOK approach essentially necessitates performing the diagnosis of the organizational processes and outlining the change requirements to handle the identified risk amicably. Seyedhoseini and Hafeti (2009) draw a comparison of RMP (Risk Management Process) with RISKIT (Risk Related to Information Technology) for software engineering, PMBOK for project

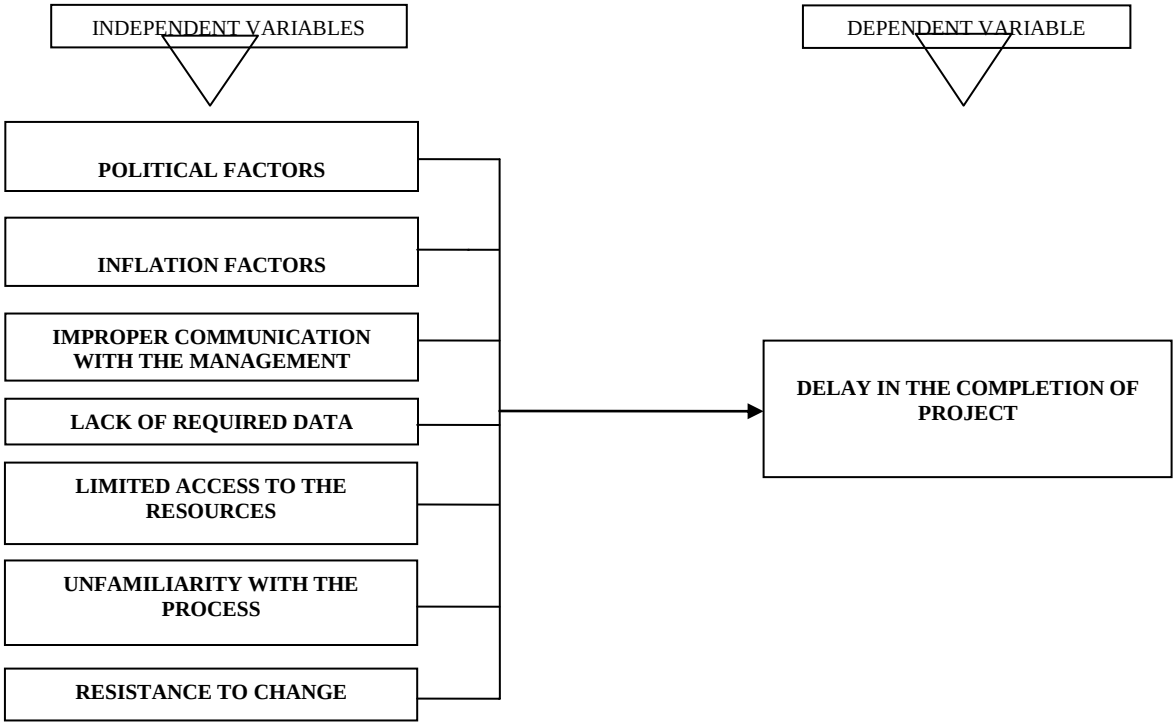
management and AS/NZS 4360 (a risk management standard) for public applications. The approaches suggested in the literature stress on assigning importance to all steps of RMP including project scope, ultimate stage of project, risk event, risk measure, risk class and response action. The TPRM framework is targeted towards use for customized project environment as the elements are derived in context with the risk and corresponding response consists of different stages, phases and steps. However, a word of caution in this regard is that performance of a project customarily depends on managers' ability to timely identify and mitigate the risks. Sources of risks can be multifaceted and risks can be cataloged based on their probability of occurrence during the project execution. The application of risk management varies for different domains and ordinarily depends on the environment in which a project is being executed (Alhawari et al., 2008).

Three major categories of events that effect the project execution include reopening, revisions and fine-tuning. A comparison of PMBOK risk management model and TPRM shows that there is no response typology in PMBOK (Seyedhoseini and Hafeti, 2009). Lack of proper resource allocation may cause failure of IT projects. Benedikt and Frank (2009) emphasize the need for continuous analysis, evaluation, monitoring and reviewing of IT projects to reduce the cost factor particularly in outsourcing of IT projects. In the same lines, Racz et al. (2010) propose a risk management methodology consisting of three stages: - orientation and scoping, model selection, analysis, and construction of integrated process model. For IT risk management, a general framework is required to be selected based on high level processes involved in risk management; and in this regard, IT compliance processes may be selected (Rath and Sponholz, 2009). The *balance scorecard* entails analyzing an organization with respect to customers, internal processes, growth, learning ability and cost related to performance. Wang et al. (2010) focus on applying *Balance Scorecard* to manage risk by measuring the performance of R&D organizations in congruence with the vision and tactics of an organization by combining *balance scorecard* with QFD in a top down fashion. Extends the basic concepts of risk analysis by performing Fault Tree Analysis (FTA) that deals with identifying all the possible risks.

FTA is opposite to FMEA as the later deals with exploring a certain event with respect to the possible risk effects. FMECA (Failure Mode Effect and Criticality Analysis) is another technique that deals with probability of failure and impact of effects; and likewise, GeoQ is another risk management approach that consist of six hierarchal phases - feasibility, pre-design, design, contracting, construction, operation and maintenance – and is used to manage all the phases of projects during the lifecycle of the project. Six Sigma tool is also used in PSP/TSP to improve the overall process performance (Park et al., 2007), but it is not an easy task as Six Sigma requires to manage altogether different type of data from different processes of PSP/TSP. In this regard, the activities of PSP/TSP are required to be identified first using selected tools, like cause and effect diagram, scatter plots, control charts, Pareto analysis and KANO analysis, in order to provide input to Six Sigma tools. The gap analysis conducted for any such model with respect to PMBOK risk management insinuates to use risk management of PMBOK. Additionally, FMEA can be used as a beneficial tool with PMBOK risk management as it has been implemented successfully in the real time environment, as well as, it identifies a number of unforeseen risks that usually result in the failure of IT projects.

Theoretical Framework and its Background: In the quest to explore factors and risks that may result in serious delays or even termination of the projects, we observe that political and inflation factors, improper communication with the management, lack of required data, limited access to the resources and unfamiliarity with the process are the core factors that could adversely affect the timely completion of the project. An elaborated review of the existing methodologies helped us to pinpoint these basic factors. In this study, we proceed with these variables as *independent variables* in order to explore the effect of these variables on the completion of a project by taking it as a *dependent variable*. We also have postulated a set of hypotheses, which we will prove in our research design to make a better understanding of the effects of independent variables over the dependent variable. Figure 1 illustrates our proposed theoretical framework.

Figure 1: Theoretical Framework



Hypotheses Development: Based on theoretical framework described in the previous section, the following hypotheses are formulated to test for their acceptance and rejection for the proposed framework.

Political Factors

H_0: Political factors have no significant relationship with the delay in the completion of the project.

H_1: Political factors have significant relationship with the delay in the completion of the project.

Inflation Factors

H_0: Inflation factors have no significant relationship with the delay in the completion of the project.

H_1: Inflation factors have significant relationship with the delay in the completion of the project.

Improper Communication with the Management

H_0: Improper communication with the management has no significant relationship with the delay in the completion of the project.

H_1: Improper communication with the management has significant relationship with the delay in the completion of the project.

Lack of Required Data

H_0: Lack of required data has no significant relationship with the delay in the completion of the project.

H_1: Lack of required data has significant relationship with the delay in the completion of the project.

Limited Access to the Resources

H_0: Limited access to the resources has no significant relationship with the delay in the completion of the project.

H_1: Limited access to the resources has significant relationship with the delay in the completion of the project.

Unfamiliarity with the Project

H_0: Unfamiliarity with the project has no significant relationship with the delay in the completion of the project.

H_1: Unfamiliarity with the project has significant relationship with the delay in the completion of the project.

Resistance to Change

H_0: Resistance to change has no significant relationship with the delay in the completion of the project.

H_1: Resistance to change has significant relationship with the delay in the completion of the project.

Formulating the Risk Equation

We define dependent variable (DP) as a function involving multiple independent variables. i.e.

DP = f (PF, IF, IC, LD, LR, UP, RC)

The independent variables identified in our study include:

- PF: Political factors
- IF: Inflation factors
- IC: Improper communication with the management
- LD: Lack of required data
- LR: Limited access to the resources and unfamiliarity with the process
- UP: Unfamiliarity with the project
- RC: Resistance to change

3. Methodology

As described earlier, risk identification and risk management are of much concern to the businesses and industrial sector; therefore, in this study we endeavor to propose a theoretical framework for risk management. The proposed framework is particularly designed to handle risks in the IT project, but it can equally be used in the various industrial and business processes. The proposed framework comprises the following phases.

Pre-Execution Processes: The trained risk management team is required to initiate the process. This team will consist of experts and trained staffs in the organization that are capable to handle the process. The next phase will be identifying the risks involved during the process and then classifying and prioritizing them according to level and impact of each risk. The trained risk management team should take real time decisions based on existing knowledge base and experience of the relevant processes to cater the risk at the right time and with lowest impact. The next phase will measure the process capability to check whether the process is capable of implementing and handling the process. Before the implementation of risk management policy, root cause analysis of the risk will be performed to arrive at certain base of taking the decision. After the root cause analysis of the process, the risk will be prioritized, implemented, controlled and monitored continuously to observe the effect of the implemented risk. It also enhances the continual improvement factor in the organization and trained team will handle and add solution to the knowledge base of the company. This phase will be used for those processes that are executing normally to check and identify the risks that can occur in the process. The sequence of activities to be carried out in the pre-execution processes is shown in Figure 2.

Post-execution Processes: Post execution will be used where the risks have been already identified and for the processes where risks have been occurred during the process in order to provide the solution in the real time environment. However, this approach would make a little difference as the trained risk management team will directly classify and prioritize the risks using the knowledge base, expert judgment and other supporting tools to handle the risk. The sequence of activities to be carried out in the post-execution processes is shown in Figure 3.

Figure 2: Pre-execution Processes

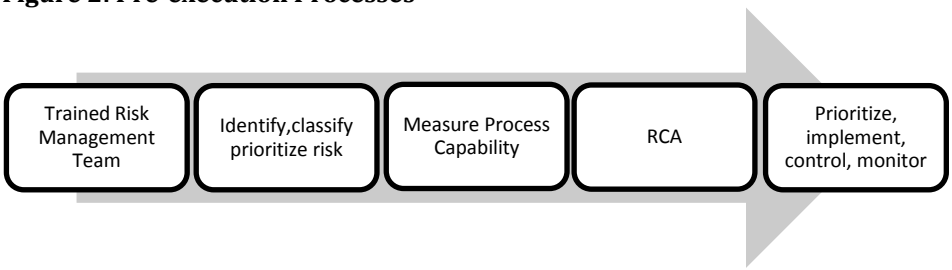
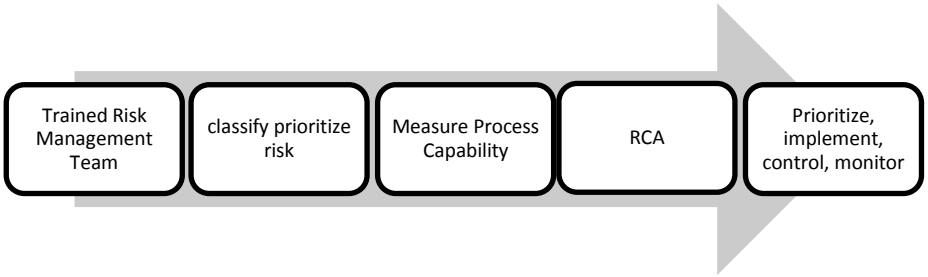


Figure 3: Post-execution Processes



Future Work: The perspective future work to this research could be to formulate a robust model for minimizing the risks associated with various business and organizational processes. Particularly, a number of processes are prone to risk related to cost, schedule and quality of the products and services. The model will be supplemented with a framework that deals with the uncertain risks and improvement of processes that are closely linked with the successful running of the project. The future perspective also covers formulation of hypothesis to validate the theoretical framework.

4. Conclusion

It is generally thought that Six Sigma is a management caprice due to which the pace of research activities in this area had always been remained at a slower pace. A data-driven process improvement undertaken using Six Sigma methodology amply caters for intrinsic risks associated with organizational and business processes. The study primarily looked into the probable methods that can be effectively adopted for risk identification within the Six Sigma framework. In this paper, we proposed a risk identification and mitigation framework for IT development using the Six Sigma methodology. The framework is formulated after an extensive critical analysis of the existing project risk handling techniques. The literature review conducted as part of the study revealed that the existing risk handling techniques are merely insufficient to account for the varied nature of the risks that are usually associated with the industrial and business processes. Though quality management aspect of Six Sigma makes it customer-satisfaction oriented approach; and the process improvement and risk management aspects make it a project management approach; hence, the core theme of Six Sigma is based on variation reduction. In view of this, the study also analyzed the key concept of Six Sigma with particular reference to quality, defect, process capability, variation and stability of operations. For this purpose, a set of hypotheses are formulated and duly tested to gauge their utility in evaluation of the risks as well as to suggest the remedial measures to mitigate these risks. The proposed framework helps identify the uncertain risks in real time environment that can be embedded in Six Sigma tools to produce quality products. The study can be beneficial to the businesses to effectively manage the probable risks associated with the projects to curtail the number of defects in the production.

References

Alhawari, S., Thabtah, F., Karadsheh, L. & Hadi, W. M. (2008). A Risk Management Model for Project Execution. In proceedings of the 9th International Business Information Management Association Conference (IBIMA), Conference on Information Management in Modern Organizations: Trends & Challenges, 887-893, January 4–6, Marrakech, Morocco.

Azizi, N. & Hashim, K. (2008). Enterprise Level IT Risk Management. Proceedings of the 8th WSEAS International Conference on APPLIED COMPUTER SCIENCE (ACS'08).

Benedikt, M. & Frank, T. (2009). Why risk management matters in it outsourcing – a systematic literature review and elements of a research agenda, 17th European Conference on Information Systems, 2009.

Deng, X. & Ma, Z. (2008). Research on risk management of large-scale software project based on consumer's demand", Proceedings of the 38th International Conference on Computers and Industrial Engineering, Oct.31-Nov.2, 2008, Beijing, China.

De-Feo, J. A. & Barnard, W. W. (2005). Juran Institute's Six-Sigma Breakthrough and Beyond: Quality Performance Breakthrough Methods. Tata McGraw-Hill Publishing Company Limited. ISBN 0-07-059881-9.

Park, Y., Choi, H. & Baik, J. (2007). A Framework for the Use of Six Sigma Tools in PSP/TSP, sera, pp.807-814, 5th ACIS International Conference on Software Engineering Research, Management & Applications (SERA 2007), 2007.

Racz, N., Weippl, E. & Seufert, A. (2010). A process model for integrated IT governance, risk, and compliance management. In: J. Barzdins & M. Kirikova (eds.), Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010. Riga: University of Latvia Press, pp. 155-170.

Rath, M. & Sponholz, R. (2009). IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen, Schmidt, Berlin

Rovai, R. L., Rodrigues, L. C. & Campanario, M. A. (2006). Strategic Model for Risk Evaluation in Project Management. IAMOT 2006.

Santos, D. & Cabral, S. (2008). FMEA and PMBOK applied to project risk management. *Journal of Information Systems and Technology Management*, 5(2), 347-364.

Seyedhoseini, S. M. & Hatefi, M. A. (2009). Two-Pillar Risk Management (TPRM): AGeneric Project Risk Management Process. *Transaction E: Industrial Engineering*,16(2), 138-148, 2009.

Zhang, W., Hill, A. V. & Gilbreath, G. H. (2009). Six Sigma: A Retrospective and Prospective Study. , POMS 20th Annual Conference, Orlando, Florida U.S.A. ,May 1 to May 4, 2009.