

## **Risk Management and Information Technology Projects**

Amine NEHARI TALET<sup>1</sup>, Razali MAT-ZIN<sup>1</sup> and Maaradj HOUARI<sup>2</sup>

<sup>1</sup>KING FAHD UNIVERSITY OF PETROLEUM & MINERALS SAUDI ARABIA

<sup>2</sup>GHARDAIA UNIVERSITY ALGERIA

KFUPM P.O. BOX 1431, DHAHRAN 31261, SAUDI ARABIA

nehari@kfupm.edu.sa

### **ABSTRACT**

IT projects management is not free from risks which are created from various sources of the environment. Thus a comprehensive understanding of these possible risks and creating strategic policies to confront them are one of the fundamental requirements for successful implementation of IT projects. The risks faced during the implementation of IT Projects are not just related to financial aspects. IT Project Managers must embrace these fundamental issues with more holistic view, rather than merely focusing on the financial matters. In order to prevent the potential problems from arising or escalating into bigger magnitude, serious attention must be given to it before the implementation of any IT project. The main focus of this paper is to investigate the impacts of Knowledge Management (KM) on Risk Management (RM) in IT project implementation process.

### **KEYWORDS**

Globalization, Information Technology, Project, Uncertainty, Risk Management (RM),

### **1. INTRODUCTION**

Knowledge has been identified as a vital source to innovative companies, a competitive advantage and value creation. It is as a key ingredient for the development of dynamic core competencies and, more generally, as a determinant factor for firms with global ambitions to meet challenges.

Firms are now forced to organize their projects and their structures. Many of them depend on their own resources or external resources to meet their objectives and be better prepared for changes in their surrounding environment.

Furthermore, firms are facing several types of risks every day due to the changes in the world environment that might introduce new risks. The source of risks differs from the internal or external environment. Uncertainty of the environment and behaviours which exert an influence on the problems in monitoring cooperation results on the level and risk of investment. If this risky environment is not managed appropriately, it might impact negatively on the present and future corporations. For this reason managers have to take into consideration risks that can affect and they have to minimize their impact on the organization.

One of the essential functions of information technology (IT) governance is risk management, which aims at providing a safe environment for E-business because IT projects are characterized by high degrees of risk.

The rapid transformation in information technologies combines changes in business processes to create surprising shifts in cost, the cost benefit relationship, and the feasibility of doing specific things in particular ways. In support of this various IT organizations, concerned with standards have published different risk management methods. These methods have been partially or fully adopted by enterprises using IT, for identifying, analysing, and minimizing risks for their IT activities.

The risks faced by IT projects are not, in essence, financial risks. By understanding these fundamental problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project. Most IT

practitioners understand that there are risks other than financial risk in projects.

IT project risk, consists of financial, technology, security, information, people, business process, management, external, and even the risk of success (which occurs when the project is so well done that it draws more transactions than expected and fails to scale to the overload requirements).

## 2. LITERATURE REVIEW

### 2.1 Risk and Uncertainty

The well-known economist [1] founder of the Chicago School, distinguishes risk from uncertainty by relating risk to a “quantity susceptible of measurement” ... “a measurable uncertainty” opposing it to real uncertainty “an immeasurable one” This reference to measurable and quantifiable events is also found within the project management literature. Risk is related to an “identifiable event that will have negative consequences whereas uncertainty relates to the source (of risk)[2]. Uncertainty is a situation being the source of risk: “a context for risks as events having a negative impact or opportunities that have beneficial impact[3]. Extending the consequence of the identified event to opportunities has the commendable intention of encouraging the management of opportunities, but adds to the confusion when trying to distinguish risk from uncertainty. A risk must contain two elements, namely uncertainty and loss [4]. RM refers to strategies, methods and supporting tools to identify, and control risk to an acceptable level [5].

Information systems projects always and everywhere around the globe have a reputation for failure, i.e. unused, partially used, cancelled and many other factors. Each project differs from another even if it is for the same system because each project has its own requirements, project management, users, organisation culture, team skills and knowledge, and many other aspects that are linked directly to the organisation and not to the project itself.

The degree of project uncertainty is an important dimension of the context. Many sources of uncertainty can be identified generating different

uncertainty levels and needing different management responses. A major source of uncertainty in IT projects is uncertainty regarding the scope or specifications of the project according to[6]. A proposed project uncertainty profile was anticipated to help determine the degree of uncertainty, from foreseeable uncertainty that can be controlled by traditional risk management techniques to unforeseeable uncertainty and chaos that may be found in some highly innovative projects[7].

### 2.2 Risk and Risk management

Risk and risk management have been studied in a variety of domains, such as Insurance, Economics, Management, Medicine, Operations Research, and Engineering. Each field addresses risk in a fashion relevant to its object of analysis, hence, adopts a particular perspective.

In some situations, risk is equated to a possible negative event as “... *events that, if they occur, represent a material threat to an entity's fortune*”[8] Using this definition, risks are the multiple undesirable events that may occur. Applied in a management context, the “entity” would be the organization. Given this perspective, risks can be managed using insurance, therefore compensating the entity if the event occurs; they can also be managed using contingency planning, thus providing a path to follow if an undesirable event occurs.

Some fields, instead of focusing on negative events, are primarily concerned with the probability of occurrence of an event. For example, medicine often focuses solely on the probability of a disease's occurrence (e.g., heart attack), since the negative consequence is death in many cases.

Finance adopts a different perspective of risk, where risk is equated to the variance of the distribution of outcomes. The extent of the variability in results (whether positive or negative) is the measure of risk. Risk is defined here as the volatility of a portfolio's value[9].

Other fields, such as casualty insurance, adopt a perspective of risk as expected loss. They define risk as the product of two functions: a loss function and a probability function.

Another important distinction in risk analysis is

the notion of endogenous versus exogenous risk. Exogenous risks are risks over which we have no control and which are not affected by our actions. Earthquakes or hurricanes are good examples of exogenous risks. Although we have some control over the extent of damage by selecting construction standards, we have no control over the occurrence of such natural events. Endogenous risks, on the other hand, are risks that are dependent on our actions.

The present study does not investigate the concept of risk per se; it is focused more on “risk management” as a practice. Project risk management is related to the set of practices and tools generally used to manage project risk. Risks in an organization can extend the range of natural disasters, security breaches, and failings of human resource, third-part vendors, financial chaos, unstable business environments and project failures. Therefore, the different types of risks encountered in common organizations.

Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). Risk is an uncertain event or condition that, if it occurs, has a positive or a negative effect on at least one project objective, such as time, cost, scope, or quality (where the project time objective is to deliver in accordance with the agreed-upon schedule; where the project cost objective is to deliver within the agreed-upon cost). A risk may have one or more causes and, if it occurs, one or more impacts. Also, risk conditions could include aspects of the project’s or organization’s environment that may contribute to project risk, such as poor project management practices, lack of integrated management systems, concurrent multiple projects, or dependency on external participants who cannot be controlled.

Furthermore, risk refers to all events, incidences and actions that may prevent you or your organization realizing its ambitions, plans and goals. Risk is surrounding us in our personal and professional lives and it is a potential problem that might happen. However, regardless of the outcome, it’s a good idea to identify risk, assess its probability of occurrence and estimate its impact.

RM is generally perceived as a way to reduce uncertainty and its consequences, which in turn will improve the chance of success. RM has the intent to take counter measures that either prevents risks or mitigates the impact of a risk. Several authors, including [10] argue that RM should form a primary part of the project management process.

RM is a distinct discipline, which integrates knowledge from a variety of other business fields. It is the discipline in which a variety of methodologies are brought to bear on a specific problem. RM is very important and integral part of any business and well recognized by the project management institutions [11]

Most projects or business venture to take place in a changeable environment in which many drawbacks exist that might negatively impact the outcome of project success. A project is considered successful if it meets the requirements determined by the stakeholders, such as security, efficiency, reliability, maintainability, functionality, integration, and other requirements [10]. A study illustrated that 35% of deserted projects are not unnecessary until the implementation stage of the project [12]. This implies that project managers are doing a poor job of identifying or terminating projects that are likely to fail due to risks encountered during the project life cycle.

The concept of the risk management is applied in all aspects of business, including planning and project risk management, health and safety, and finance. It is also a very common term amongst those concerned with Information Technology. A generic definition of risk management is the assessment and mitigation of potential issues that are a threat to a business, whatever their source or origin. [13].

The concept is now fairly universally understood, having been in widespread use for a number of years. It is applied in all aspects of business.

To discuss the definition of the risk management is necessary to explain in advance the meaning of the three main concepts:

Threat is the potential cause of an unwanted impact on a system or organization (**ISO 13335-1**). Threat can also be defined as an undesired

event (intentional or unintentional) that may cause damage to the goods of the organization.

Vulnerability is a weakness in system procedures, architectural system, its implementation, internal control and other causes that can be exploited to bypass security systems and unauthorized access to information. Vulnerability represents any weakness, administrative process, act or statement that makes information about an asset to be capable of being exploited by a threat.

Risk management is a process consisting of:

- Identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives;
- Risk assessment by setting the probability and impact of its production, following threats by exploiting vulnerabilities;
- Identify possible countermeasures and deciding which one could be applied, in order to reduce the risk to an acceptable level, based on the value of information resource to the organization.

RM is concerned with identifying risks, understanding risks and drawing up plans to minimize their effect on project. RM can be seen as a series of steps that help a software team to understand and manage uncertainty [14].

RM objective is to identify all applicable risks in a project or business or product. It involves ranking the above elements based on their importance, frequency of occurrence, level of impact and then establishes the actions needed to control the identified risks. It is possible for every individual risk aspect to be documented in further details [15]. Since no one can predict what losses will occur, the objective of RM is to ensure that no risk will occur during the execution of a project in order to minimize losses to an acceptable level. If a loss occurs, then the objective of RM has failed to achieve the objectives intended, which prevent the organization from pursuing their goals.

The goal of performing risk management is to enable the organization to maintain at the highest values the activity results. This process should combine as efficient as possible, all factors which can increase the probability of success and

decrease the uncertainty of achieving objectives. Risk management should be an evolving process. Particular attention should be given to the implementation of the strategies for eliminating or reduce the risk and their appliance, to the analysis of the past evolution of risks and to the present and future prediction of the events. Management process should be implemented at the highest management level.

The link between uncertainty and failure (or between certainty and success) seems to be well established, but the link between risk management and success is not as clear. Clear indications are presented of the influence of individual project risk management activities on the success of IT projects[16].

In IT one of the most important goals of risk management is to accomplish by better securing the informatics systems that store, process, or transmit organizational information; by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget and by assisting management in authorizing (or accrediting) the IT systems, on the basis of the supporting documentation resulting from the performance of risk management.

### 2.3 Risk Management Process

Risk management is a permanent cycle process that involves activities for establishing, monitoring and ensuring continual improvement of the organization's activity. This process includes four main activities, which have to be permanent applied and developed:

- *Design the management system* involves identifying business requirements, assessing the likelihood and the impact of the risks, including the implementation of a security policy and selecting the adequate countermeasures for the existing risks;
- *Implement the management system* involves applying control measures and work procedures, resource allocation, setting the responsibilities and conduct training and awareness programs;
- *Monitoring, reviewing and reassessing the management system* involve an

evaluation of effectiveness of controls and working procedures, of business changes, of previous incident reports and of existent risks;

- *The improvement and update of the management system* involves correcting the identified dysfunctions, or eliminating the unsustainable decisions or applying new control measures.

Risk management encompasses three processes:

1. Risk assessment is the process comprises establishing criteria under which the evaluation takes place (procedure on existing threats and vulnerabilities, and risks associated with, proceedings concerning the impact and likelihood of identified risks, risk assessment procedures, procedures for identifying measures to mitigate or eliminate risks, procedure for selecting the best measures to mitigate or eliminate the risks) and identifying and assessing risks..

2. Risk mitigation refers to determining optimal measures to eliminate or mitigate the risks, to planning, implementing the optimized selected measures, according to the plan, and controlling the rightfulness of the implementation process.
3. Reassessment of the residual risk consist of evaluating the remaining risk after the risk mitigation step and determine whether it is an acceptable level or whether additional measures should be implemented to further reduce or eliminate the residual risk, before the organization can perform work properly.

There are types of RM processes used in organizations today. These are summed up in Table 1. The processes of RM have emerged in a number of existing process models in the area of RM.

Table 1: The processes of Risk Management from previous studies

Main Dimension/ RM Process	Description of Process						References
	1	2	3	4	5	6	
Software development process	Risk identification	Risk analysis	Risk control planning	Risk monitoring			[17]
Software risk management	Risk Identification	Risk Analyze	Risk Plan	Risk Track	Risk Control		[18]
Role in software engineering	Review Define Goals	Risk Identification	Risk Control Planning	Risk Analysis	Risk Control	Risk Monitoring	[19]
RM as verification and validation	Risk Identification	Risk Analysis	Risk Planning	Risk Tracking	Risk Control		[20]
Software project management	Risk Identification	Risk Analysis	Risk Prioritization				[21]
Software development	Risk Identification	Risk analysis	Risk monitoring				[14]
Data warehouse system	Goal definition review	Risk Identification	Risk Analysis	Risk Planning	Risk Tracking	Risk Control	[5]
RM in insurance field.	Risk Identification	Risk Evaluation	Risk Evaluation	Risk Monitoring			[22]
Controlling product development	Identify Risks	Analyze Risks	Prioritize and map risk	Resolve Risks			[23]
Project management	RM planning	Qualitative risk analysis	Quantitative risk analysis	Risk response planning	Risk monitoring and control		[24]
Software engineering	Risk Identification	Risk Analysis	Risk Planning	Risk Monitoring			[25]
Software Risk Management Process	Plan and implement risk management	Manage the project risk profile	Perform risk analysis	Perform risk monitoring	Perform risk treatment	Evaluate RM process	[26]
Risk architecture	Risk classification	Risk identification	Initial risk assessment	Risk mitigation	Risk monitoring		[27]

RM involves the following stages:

- 1) Risk Identification is to identify project, product and business risks;
- 2) Risk Analysis is to assess the likelihood and consequences of these risks;
- 3) Risk Planning is to draw up plans to

avoid or minimize the effects of the risk; and 4) Risk Monitoring is to guarantee the effectiveness of the methods followed and to monitor the risks throughout the project. Figure 1 illustrates the proposed Risk it method [19].

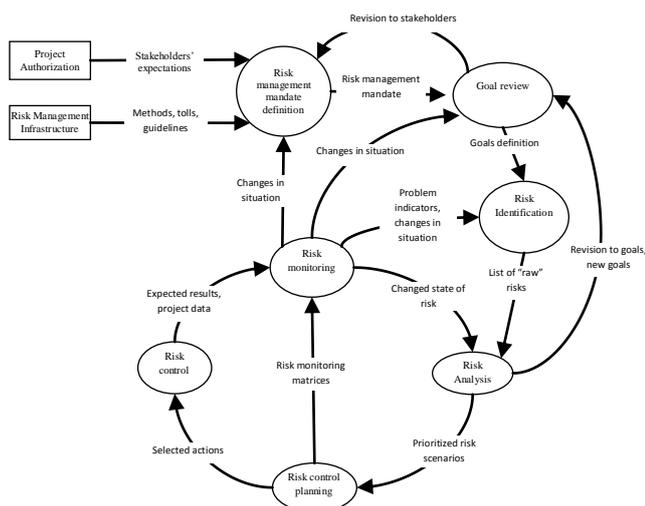


Figure 1: Riskit RM Cycle[19]

From figure 1 RM process is divided into Risk Identification, which focuses on a variety of technological content, environmental communication execution and operation approaches, programmatic constraints and the mission duration[20]. The second is Risk Analysis of the consequences of the possible risks by scoring their impact on the necessities should they occur.

The third is Risk Control, which is deciding the best suitable and cost-effective measures needed to be executed in order to control the risks such as risk avoidance, risk reduction, and risk transfer. The fourth is Risk Monitoring, which provides a review of the organization's ability to deal with incidents that might result in business interruption, implementing risk identification, Evaluation and Control measures that minimize the likelihood and severity - both in terms of potential financial and reputation losses of an incident, but can never entirely eliminate the risks. The result is a requirement-driven risk list where failures are listed based on their impact on weighted requirements. Risk planning process has design rules, process controls, testing, modeling, and inheritance. Risk Tracking contains a tool to display the number of report formats to be used by different personnel for different reasons. Risk Control is designed for implementation, which allows the project team to effectively control risk and watch its growth or decline as the design evolves and the results of implementation become available.

RM process is described into six steps:

- 1) Goal Definition: review the stated goals for the project, refine them and define implicit goals and constraints explicitly.
  - 2) Identification: identify potential threats to the project using multiple approaches.
  - 3) Analysis: classify risks, complete risk scenarios, estimate risk effects and estimate probabilities and utility losses for risk scenarios.
  - 4) Control and Planning: select the most important risks, propose controlling actions and the actions for implementation.
  - 5) Control: implement the risk controlling actions.
  - 6) Monitoring: monitor the risk situation
- Figure 2 illustrates the RM process [28].

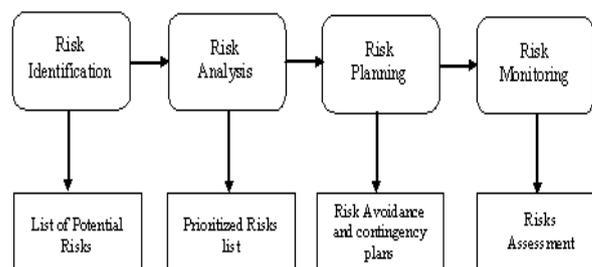


Figure 2: RM Processes [28]

RM process contains the following processes: identifying risks using brainstorming techniques to discover any risks that prevent the progress of the project, analyzing risks by the team members to determine if a certain risk is worth migrating or not, prioritizing and mapping risk to establish a seriousness of the risk according to their impact, and resolving risks by implementing plans to prevent risk from occurring [29].

## 2.4 Sources of Risks in IT projects

By examining the literature reviews, IT projects can range from software development, outsourcing, communications and implementing a new security infrastructure. Also, these IT project risks might have a particular management in a different project. Risks are resulting of many factors involved in the projects. Each factor will depend on the type and purpose of the project.

IT projects are characterized by high degrees of risk. The rapid pace of change in technologies combines changes in business processes to create unpredictable shifts in cost,

the cost benefit relationship, and the feasibility of doing specific things in particular ways [30].

One classic problem identified in many IT projects occurs when new technologies are developed as the project is underway [31].

A survey of more than a thousand Canadian organizations found that the main reason for IT project failure was inadequate risk management and a weak project plan. The risks faced by IT projects are not, in substance, financial risks [32]. The financial measures are only indicators of the underlying problems. By understanding these underlying problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project. Most IT practitioners understand that there are risks other than financial risk in projects.

IT project risk are broken into nine categories, including financial risk, technology risk, security risk, information risk, people risk, business process risk, management risk, external risk, and even the risk of success (which occurs when the project is so well done that it draws more transactions than expected and fails to scale to the overload requirements[33].

Anecdotes, surveys, and field research studies establish that many IT projects fail. Managers abandon some of these failing systems. Other projects that are over budget or behind schedule ultimately result in useful systems [34]. However, many more projects continue long after any hope of success has faded[35]; [36].

IT projects are much more likely to fail than other types of projects, such as building construction projects and states that the main causes for IT project failures are their use of rapidly changing technologies, their generally long development times, and the volatility of user expectations about what the project will yield. Because IT projects generally include all of these characteristics, they are prone to failure, cost overruns, and schedule delays [37].

Organizations need to keep IT projects on schedule and costs under control. However, organizations must also encourage managers to respond to changing business needs and exploit technological opportunities before their competitors do so [38].

In terms of IT projects, risks can vary, whether it is a software development project, security project, outsourcing project, or specific programming task.

IT projects are known for their high failure rate. Based on in-depth interviews with IT professionals from leading organizations in Western Australia were undertaken to determine how IT risks were managed in their projects. The respondents ranked 27 IT risks in terms of likelihood and consequences to identify the most important risks[39]. The top five risks, in order, are: personnel shortfalls; unreasonable project schedule and budget; unrealistic expectations; incomplete requirements; and diminished window of opportunity due to late delivery of software. Furthermore, the respondents overwhelmingly applied the treatment strategy of risk reduction to manage these risks. Additionally, these strategies are primarily project management processes, rather than technical processes. Therefore, this demonstrates that project management is a RM strategy. In particular, managing stakeholders' expectations is a specific risk treatment that helps to manage several key IT risks[39].

The risk issues in reference to software development process are not viewed as essential subject of discussion. On the other hand, most organizations hope to implement systems successfully while still assuming their regular business processes. Yet, new systems are not implemented in a space and many authors concur that the first step in developing a business continuation plan is to carry out a risk assessment [40].

There are different types of risks and each depends on the kind of IT project involved. Risks can vary whether it is a software development project, or security project, or outsourcing project, or specific programming task. By investigating the effects of risk management on IS/IT project success, it was concluded that project risk management is defined in the literature as being an instrumental action based on rational problem solving.

The purpose of RM is to develop a detail analysis of the project and to establish a comprehensive list of risks.

RM assists project team to make better

decisions, communication and to resolve any risk issues in effective matter.

## ACKNOWLEDGEMENTS

The first two authors are grateful to King Fahd university of Petroleum & Minerals for its continuous support **Project: SB111010**

## Bibliography

- [1] H. Knight. (1921) Risk, Uncertainty and Profit. [Online]. [www.econlib.org/library/Knight/knRUP.html](http://www.econlib.org/library/Knight/knRUP.html)
- [2] Sicotte, H. & Bourgault, M., "Dimensions of uncertainty and their moderating effect on new product development project performance," *R&D Management*, vol. 38, no. 5, pp. 468-79, 2008.
- [3] B. E. Perrott, "'A strategic risk approach to knowledge management'," *Business Horizons*, vol. 50, no. 6, pp. 523-533, 2007.
- [4] Parvatiyar, A., & Sheth, N., "Customer Relationship Management: Emerging Practice, Process, and Discipline.," *Journal of Economic and Social Research*, vol. 3, no. 2, pp. 1-34, 2001.
- [5] Bruckner, M., List, B., & Schiefer, J., "Risk-Management for Data Warehouse Systems," *Data Warehousing and Knowledge*, pp. 219-229, 2001.
- [6] L. Kumar, "Managing risks in IT projects: an options perspective," *Information & Management*, vol. 40, pp. 63-74., 2002.
- [7] Meyer, A., De, C., Loch, H. and Rich, M.T., "Managing project uncertainty: from variation to chaos," *MIT Sloan Manage. Review*, vol. 43, no. 2, pp. 60-67, 2002.
- [8] M. and Schneider, M. Levin, "Making the Distinction: Risk Management, Risk Exposure," *Risk Management*, vol. 44, no. 8, pp. 36-42, 1997.
- [9] E. Levine, "Defining Risks," *CA Magazine*, vol. 133, no. 3, pp. 45-46, April 2000.
- [10] Powell, P. L., & Kelin, J. H., "Risk Management for Information Systems Development," *Journal of Information Technology*, pp. 309-319, 1996.
- [11] Del Cano, D., & Cruz, P. , "Integrated Methodology for Project Risk Management," *Journal of Construction Engineering and Management*, vol. 128, no. 6, pp. 473-485, 2002.
- [12] Ewusi-Mensah, K., & Przasnyski, H. , "On Information Systems Project Abandonment:An Exploratory Study of Organizational Practice.," *MIS Quarterly*, vol. 15, no. 1, pp. 67-88, 1991.
- [13] Southern, S. , "Creating risk management strategies for IT security," *Network Security*, pp. 13-14, 2009.
- [14] Bandyopadhyay, K., Myktyun, P., & Myktyun, K. , "A framework for integrated risk management in information technology.," *Management Decision*, pp. 437-444, 1999.
- [15] Cule, P., Schmidt, R., Lyytinen, K., & Keil, M. , "Strategies for Leading off is Project Failure," *Information Systems Management*, vol. 14, no. 2, pp. 68-73, 2000.
- [16] Bakker, K., Boonstra, A. and Wortmann, H. , "How risk management influences IT project success," in *IRNOP IX Conference 2010*, Berlin, Germany, 2009.
- [17] Boehm, B., & Bose, P. , "A collaborative spiral software process model based on theory W," in *3rd International Conference on the Software Process (ICSP94)*, New York, 1994.
- [18] Higuera.R & Haimes.Y, "Software Risk Management," Software Engineering Institute Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, Technical Report CMU/SEI-96-TR-012 ESC-TR-96-012, 1996.
- [19] J. Kontio, "The Riskit Method for Software Risk Management version 1, 00," University of Maryland. College Park, MD, Computer Science Technical Reports CS-TR-3782 / UMIACSTR- 97-38, 1997.
- [20] S., Feather, M., & Hicks, K. Cornford, "DDPTool for life-Cycle Risk Management. Jet Propulsion Laboratory," California Institutte of Technology, IEEE, 2001.
- [21] J., Jurison, "Software projectmanagement: The manager's view. ," *Communications of Association for Information Systems*, vol. 2, no. 17, pp. 2-52, 1999.
- [22] Beck, T., Levine, R., Loayza N., "Finance and the Sources of Growth," *Journal of Finance and Economics*, vol. 58, pp. 261-300, 2000.
- [23] P. & Merritt, G. Smith, "Proactive Risk Management: Controlling Uncertainty in Product Development," *Productivity Press, New York*, 2002.
- [24] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* , 4th ed., 2008. [Online]. <http://www.projectsmart.co.uk/pdf/pmbok.pdf>
- [25] Sommerville. I, *Software Engineering*, 8th ed. University of St. Andrews, , United Kingdom: Addison-Wesley, 2006.
- [26] Software & Systems Engineering Standards Committee of the IEEE Computer Society, "Systems and software engineering — Life cycle processes — Risk management ," International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 16085 IEEE Std 16085-2006, ISO/IEC 16085:2006(E) IEEE Std 16085-2006, 2006.
- [27] TOGAF. (2009) The Open Group Architecture Framework (TOGAF). [Online]. [http://www.kingdee.com/news/subject/10togaf/pdf/TOGAF\\_9\\_ziyuan.pdf](http://www.kingdee.com/news/subject/10togaf/pdf/TOGAF_9_ziyuan.pdf)
- [28] I. Sommerville, *Software Engineering*, 6th ed.: Addison-Wesley, 2001.
- [29] Smith, G. & Merritt, M. , *Proactive Risk Management: Controlling Uncertainty in Product Development.*: Productivity Press., 2002.
- [30] K. Schwalbe, *Information technology project*

*management*. Boston: Course Technology, 2007.

- [31] H. Havenstein, "IT execs seek new ways to justify Web 2.0," *Computerworld*, vol. 41, no. 33, pp. 14-15, 2007.
- [32] B. Whittaker, "What went wrong? Unsuccessful information technology projects.," *Information Management & Computer Security*, vol. 7, no. 1, pp. 23-29, 1999.
- [33] McKeen, J. & Smith, H. , *Making IT happen: Critical issues in IT management*. West Sussex, England: Wiley, Ltd, 2003.
- [34] G. Anthes, "SEC electronic filing system in high gear," *Computerworld*, vol. 27, pp. 59-67, 1993.
- [35] J. Johnson, *Chaos: The dollar drain of IT project failures.*: Application Development Trends, 1995, vol. 2.
- [36] M. & Sabherwal, R. Newman, "Determinants of commitment to information systems development: A longitudinal investigation.," *MIS Quarterly*, vol. 20, pp. 23-54, 1996.
- [37] G., Lane, S., & Bruton, C Schneider, "Monitoring risk in information.," vol. 13, no. 1, pp. 63-67., 2009.
- [38] S. Murthi, "Managing the strategic IT project, Intelligent Enterprise," vol. 5, no. 18, pp. 49-52, 2002.
- [39] D., Salm, G., & Love, D. Baccarini, "Management of risks in information technology projects," *Industrial Management & Data Systems*, vol. 104, no. 4, pp. 286-295, 2004.
- [40] S. Maguire, "Identifying Risks during Information System Development: Managing the Process," *Information Management and Computer Security*, vol. 10, no. 3, pp. 126-137, 2002.