DOI: 10.7763/IPEDR. 2014. V69. 6

Incorporation of Knowledge Management with Risk Management and Its Impact on Is/It Projects

Amine Nehari Talet[1+] and M. Zakaria Nehari Talet[2]

[1] King Fahd University of petroleum & Minerals, Saudi Arabia

[2] Telfer School of Management- University of Ottawa, Canada

Abstract. Information systems are the fundamental of today's promising businesses. Billions of dollars are exchanged on daily basis based on automated systems and information technology. It is crucial that information system projects are properly scope and implemented successfully.

Different research and studies, regarding information systems or information technology project failure show the highest risk factors that were behind the project failure. The world statistics always publish failure rate in general, which clearly can prove for business and information technology executives that there is failure at IS projects regardless of whether it is high or low for (IS) or (IT) projects. The key objective of all the research and studies is information and communications technology awareness which can reduce or resolve failure rate for a project by using the accurate and professional techniques.

This paper will present a Knowledge-Based Risk Management KBRM process conceptual framework and its impact on IS/IT projects. It will introduce the role of knowledge management support for risk management processes to anticipate on IT project.

Keywords: Knowledge Management (KM), Risk Management (RM), Information Systems (IS), Project.

1. Introduction

The project risk management process, as described in project management handbooks, is an example of a rational problem-solving method [1] based on an instrumental view. For this process to be effective, it is necessary to follow all prescribed steps. For example, it has been have shown that the prescribed sequence of risk identification, risk analysis, planning actions, and executing actions is rarely followed [2], [3]. The sequence of activities that characterizes project risk management consists of identifying risks, analyzing risks, defining action, implementing action, and monitoring the situation. However, despite the recommendation to employ risk management, there are indications in literature that risk management used in Information Systems/Information Technology (IS/IT) projects only occasionally contributes to project success [4]. Nevertheless, project managers often choose to execute various risk management activities in their projects [3], [2], in order to manage their risks and uncertainties [5]. Execution of these activities, for instance risk identification or risk analysis, requires time and cost money, and therefore they consume part of valuable project resources. In order to improve the success of the project, these resources could also be expended elsewhere, for instance to perform additional testing of the IS/IT system.

2. The Role of Knowledge Management Process &Risk Management in IS Projects

KM and its Risk require significant attention within the majority of twenty-first century organizations. The purpose is to obtain the most comprehensive, completed and relevant information of risks to be able to respond rapidly to the environment surrounding the organization. Nowadays, organizations are surrounded by turbulent environment, which might change and initiate new risks. Therefore, organizations must arm themselves with comprehensive knowledge to be able to face the risks introduced by the unstable environment. Additionally, Knowledge risk management (KRM) is an emerging field which suggests a solution to the problems connected with conventional risk management methods [6]. The problem of environmental complexity is manifested by individuals not knowing enough about the risk to anticipate its

[+]Corresponding author. Tel:+ 00966138603450.

E-mail address: nehari@kfupm.edu.sa.

likelihood and consequences. To improve RM processes, the researchers will examine the relation between KM processes and RM processes. The objective is to introduce the Knowledge-Based Risk Management (KBRM) process to improve RM process efficiency by employing some of KM process. The project risk management process, as described in project management handbooks, is an example of a rational problem-solving method [7], based on an instrumental view. For this process to be effective, it is necessary to follow all prescribed steps. For example, the prescribed sequence of risk identification, risk analysis, planning actions, and executing actions is rarely followed [2] and [3]. Based on research conducted, an effective RM process model can't be achieved without the assistant of a well-established KM process model [8]. In another study, KM as a discipline can add positively to RM implementation in reference to data and information management, risk-knowledge sharing and analysis consolidation and reporting[9]. Risk Management is becoming a key factor within organizations since it can minimize the probability and impact of IT project threats and capture the opportunities that could occur during the IT project life cycle.

KM processes as well have turned out to become a strategic resource for the organizations. KM can have a great influence on reducing organizations' risks [10]. However, using KM processes to improve the application of RM processes is a recent and significant research area. In spite of its importance, this area of research has not been addressed intensively up to now. A company cannot manage its risks effectively if it cannot manage its knowledge, many projects failed due to lack of knowledge among the project team or lack of knowledge sharing during project progress [11]. A project failure can be the result of capturing the appropriate knowledge at an inappropriate time of the project [12]. In fact, without KM as a tool to communicate risks among members of a project team, RM might suffer from ineffectiveness and inefficiencies [13]. A KM framework was developed to utilize when performing a task is based on approach to KM and assumes that knowledge is created, transferred and reused due to an individual performing a specific task [14]. Since knowledge is created in a project by the project team member completing the task. Therefore, an organization needs to ensure that knowledge from one project is available for use on future projects to reduce rework. Furthermore, the application of KM processes to support RM processes has the potential of iteratively mitigating the probability of risks, thereby raising the probability of successful project execution [12]. It is important that the organization prioritizes knowledge infusion of RM which, would require the creation, capturing and sharing of knowledge related to potential risks to key assets of stakeholders. The key to proactive RM processes lies in the company's ability to mobilize the knowledge and expertise of its employees regarding risk mitigation to provide the organization's decision makers an accurate and timely information about potential harmful incidents, for example [11]. The rationale for applying KM techniques and risk programs is stated in the following: 1) Sensing and responding to risks in an organization is very much dependent on the knowledge and judgment of employees at all levels. 2) Key decision makers should mobilize this knowledge along with any other information available concerning potentially threatening situations. 3) Utilizing KM techniques through opening communication channels to provide a system of incentives for managers to encourage employees to uncover potentially dangerous issues. Finally, 4) Capturing lessons learned, applying proven RM techniques, and creating decision support systems to assist in developing preventive RM policies and to avoid costly repetition of errors.

The Hobart City Council in Tasmania, Australia conducted a pilot information audit to establish the current state of information management in the Council, as part of its KM strategy. This resulted in an audit report of RM activities containing audit tables as a KM reference capability. It has improved the understanding and application of information and KM in the Council [15]. Moreover, the audit has identified the gaps and duplications as well as examples of best practices in information and knowledge management across the organization. In another study three core KM principles related to RM have been noted [16]. These are: business focus, accountability and operational support. The three KM principles can be applied to information RM in order to generate risk intelligence and to maximize the return on value from information RM (investments. Business focus includes five steps: 1) Start with key business risks, 2) Prioritize the business risks based on their importance to the business strategy, 3) Identify information sources for the high-business risk areas, 4) Identify at-risk information sources through establishing what information is critical to the business process, and 5) Establish risk-mitigation strategies. Furthermore, KM accountability

requires domain experts to be assigned to work with knowledge managers to maintain various information sources [16].

Finally, operational support is required to obtain the value. In addition, an effective RM is built on effective KM, which necessitates open, obvious and enduring communication within the team involved [17]. Our proposed KBRM framework for IT project was designed based on a thorough investigation of various models presented by different authors. A new methodology that contributes in providing guidance for developing risk modelling knowledge was introduced to improve the quality and quantity of RM processes. As shown in Fig. 1, they claimed that in three key components of ERM (Enterprise Risk Management) there are relations between data, search of problem solutions, policies and organization of outcomes such as risk [8].

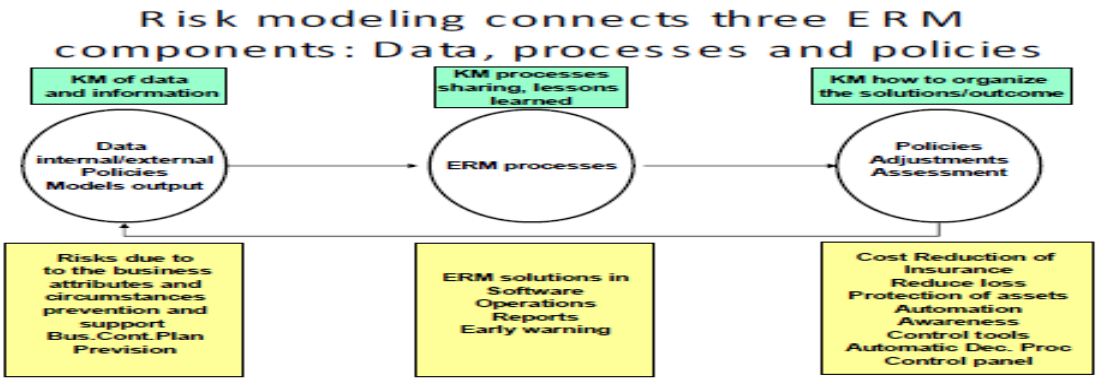

Fig.1: Knowledge management acts through risk modelling in different components of enterprise risk management processes in [8].

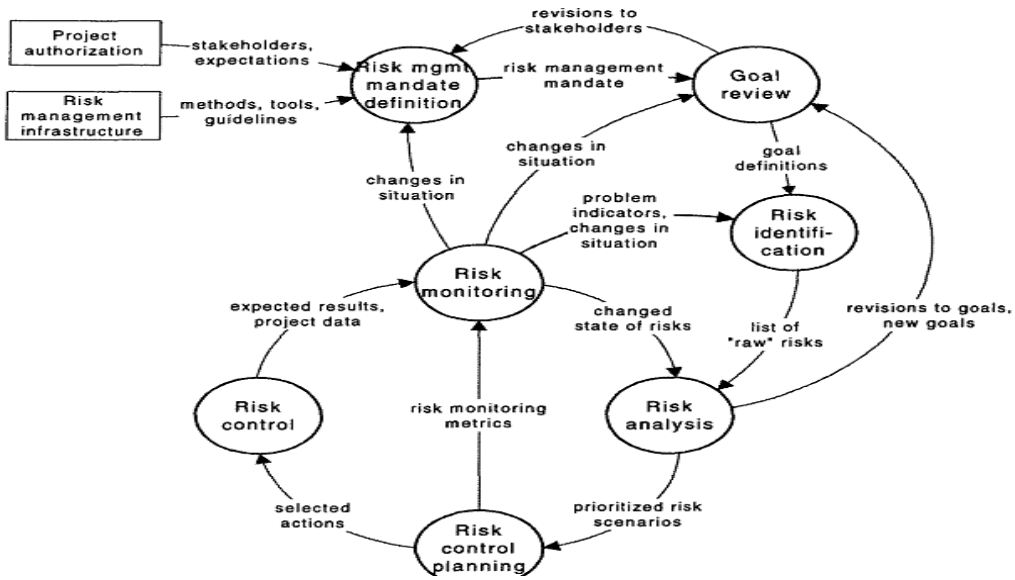

Fig. 2: Riskit RM cycle [19].

As a result, their proposed methodology used the context and experience to improve the risk modeling process and it's composed of the following steps: 1) Answering questions related to the strategy and strategic planning. 2) Determining the enablers to transfer risk knowledge from tacit to explicit knowledge and vice versa. 3) Producing knowledge by understanding the information flows. 4) Understanding risk knowledge organization. 5) Finding out KM technologies and techniques. 6) Designing the Enterprise Risk KM System to support risk modeling. 7) Finally, connecting organizational performance metrics and risk modeling.

Another interesting research in managing knowledge risks in which a coherent methodology for managing risks [18]. The proposed methodology can help in facilitating effective RM processes and enabling all project participants to develop and share a greater understanding of project risks. The methodology includes a generic process model, underlying information model, fuzzy knowledge representation model and common language for describing risks and corrective actions, in order to support the quantitative risk analysis and prototype software implementation. A comprehensive RM tool called IRMAS (Intelligent Risk Mapping and Assessment System).

Several authors have mentioned the risks encountered during IT projects and how KM might play an important role in enhancing the execution of RM. Most authors recognized how well integrated KM and RM models are crucial to improve IT projects executions. However, none of the authors defined a clear and comprehensive framework to demonstrate how to integrate the KM and RM processes together.

2.1 KM risk identification

RM has become the main part of the organization activity and its main objective is to help all other activities to reach the organizations aim directly and efficiently. It is a continuous process that depends directly on the change in the internal and external environment requires continuous attention for identification and control of risk [20].

A proposed an integrated risk management model for financial banks with knowledge management recommend that the financial banks should set up the incentive mechanism to urge the staffs to learn more knowledge, and at the same time, banks should train knowledgeable staffs to construct a whole system to assess and calculate the potential risks and counter-measures to reduce risks and feedback [21].

The literature of knowledge management recognizes the importance of two concepts: relating knowledge management to business goals, and analysing existing knowledge and information management practices to identify gaps. Like other business processes, knowledge management needs to address the business needs within an organization and to encompass set goals and priorities for delivering benefits [22]. The new field of knowledge risk management (KRM) offers managers ways to use knowledge to make sure decision makers is informed and can anticipate and respond to risk events [6].

Risk identification, which covers the identification within the established context of uncertain events that could cause harm or benefits, associated causes and the potential consequences [23]. RI is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern; or it can be the process of identifying probable effective risk factors in relation to project goals, determining their features, and finally documentation of findings. In addition, it is defined as obtaining the right information for the right people at the right time to help them in problem-solving [24]. Project managers can take appropriate action if proper risk assessment leads to early identification of a failing project.

The globalization and the technological development in the business sector forced business organizations to cooperate on a broader scale. The knowledge of cooperation and the risks into cooperation have become fundamental to business success [25]. In addition, correct risk identification ensured risk management effectiveness. A project failure can be the result of capturing the appropriate knowledge at an inappropriate time of the project [26]. In fact, without KM as a tool to communicate risks among members of a project team, RM might suffer from ineffectiveness and inefficiencies [27]. It appears that is not sufficient to augment current Information Security Risk Assessments (ISRAs) methodologies merely by including the identification of “knowledge assets” in the form of databases, or even key people [28]. Certainly, a complex organizational process tends to rely on both explicit and tacit knowledge of various individuals and networks of experts. Therefore, understanding the full spectrum of risks associated with a particular process extends considerably beyond individuals and information assets alone. This line of thought suggests that if we wish to consider knowledge as a possible source of risk, the asset-based risk identification approach is likely to be insufficient [28]. Information security is the dominant to organizations, so ISRAs enable organizations to identify their key information assets and risks in order to develop effective and economically-viable control strategies[29].

In order to be effective, RM should involve the following stages: 1) Risk Identification: used to identify project, product and business risks.2) Risk Analysis: to assess the likelihood and consequences of these risks. 3) Risk planning: to draw up plans to avoid or minimize the effects of the risk. 4) Risk Monitoring: to guarantee the effectiveness of the methods followed and to monitor the risks throughout the project [30]. Also, in RM process, the team shares their knowledge on selecting the best alternative for risk treatment in risk action requests. Whenever a risk treatment alternative is recommended in a risk action request, an evaluation should be made by the stakeholders to determine if the risk is acceptable, then a risk treatment alternative should be implemented, supported by the necessary resources, monitored and coordinated with other project activities. A framework of the knowledge-based supply chain risk management system was developed which includes four modules: basic database, knowledge database management, and supply chain risk early warning and risk management strategies module [31].

2.2 KM and risk analysis

Risk analysis is concerned with assessing the potential impact of exposure and likelihood of the particular outcome actually occurring. The impact of exposure should be considered under the elements of time, quality, benefit and resource. A high number of IT projects failures have put RM higher in the agenda of prospective project management teams. These failures created a major pressure on the system developers to try harder and take the risk out of IT implementation [32]. He points out that there are many risk factors to consider before the IS goes live at the end of the project. Some risk factors can include for example, risk associated with new technology, project size and failure. Since there are many things that might go wrong during the process of system development, organizations should simultaneously attempt to reduce risk and increase security during system implementation. He recommends risk assessment to be performed at the start of a project, and at least before system design, to determine the level of risk and to create a plan to manage them. Furthermore, he concludes based on the use of a live case study that there is a need to develop a risk analysis methodology that incorporates the key issues that need to be addressed before a system goes live. Risk analysis facilitates the conversion of risk data into decision making information [33]. It consists of the following tasks: 1) Risks shall be identified in the categories described in the risk management context. 2) The probability of occurrence and consequences of each risk identified shall be estimated. 3) Each risk shall be evaluated against its risk thresholds. 4) For each risk that is above its risk threshold, recommended treatment strategies shall be defined and documented as recommended by IEEE Computer Society, 2008. Therefore, based on the confirmed risks identified in the previous stage, risk analysis will perform analysis on each risk. The team members will share their experience on confirmed risks based on probability of occurrence, impact and extend of loss. This phase can be divided into risk probability which 1) describes the likelihood of events occurring. 2) Shows the risk impact to measure the severity of risk. 3) Displays the extent of loss to determine the risk disclosure in order to list all risks and threats [34]. The probability of occurrence and consequences of each risk identified should be estimated. The estimates can be quantitative or qualitative depending on the organization. The stakeholders should share their knowledge in determining which risks will be evaluated using a qualitative scale and which will be evaluated using a quantitative scale. During the risk analysis, the data collected is being renovated into decision making information [35]. Also, risk analysis will categorize the risks based on the likelihood of occurrence, impact and extend of loss [33]. Also, in RM process, the team shares their knowledge on selecting the best alternative for risk treatment in risk action requests. Whenever a risk treatment alternative is recommended in a risk action request, an evaluation shall be made by the stakeholders to determine if the risk is acceptable. If the stakeholders determine that actions should be taken to make a risk acceptable, then a risk treatment alternative shall be implemented, supported by the necessary resources, monitored and coordinated with other project activities [35].Techniques for Risk Analysis include [34]. (1)Best practice, alert system and lessens-learned; (2) Expertise locator might be needed to share tacit and explicit knowledge; (3) Risk Modeling to transfer knowledge through presentation, portals, discussions, collaboration activities and testing reporting.; (4) Review case studies from previous projects; (5); Quick evidence review (QER) to review research and evidence on a particular issue; (6) Gone well/not gone well Tools; (7) Team discussion and brainstorming performed by analyzing former projects accessed from the repository.

Another research examined the relationship between knowledge and risk analysis is described in [18]. It presents a coherent methodology for managing risks. The proposed methodology can help in facilitating effective RM processes and enabling all project participants to develop and share a greater understanding of project risks. The methodology includes a generic process model, underlying information model, fuzzy knowledge representation model and common language for describing risks and corrective actions, in order to support the quantitative risk analysis and prototype software implementation.

A framework of the knowledge-based supply chain risk management system was developed in which it focuses on utilizing knowledge management theories and data mining methods to supply chain risk management and set up framework of the knowledge-based supply chain risk management system [31].

2.3 KM and risk planning

Risk Response Planning assists in converting the knowledge of risk into action and judgment and involves developing actions to deal with each risk, prioritizing measures and creating a management plan[33]. This phase takes the information collected to formulate plans, strategies and actions and its ultimate goal is to reduce both the probability of risk occurring and the degree of that loss [36]. The Risk Response Planning process recommends the risk treatment actions needed in the later stages and requires selecting the proper security control methods according to the impact and the probability of risks. This phase also provides different execution possibilities and examines different "What-if" options. According to Project Management Institute [37], Risk Response Planning is the process of developing options and determining actions to enhance opportunities and reduce threats to the project's objectives. It includes the identification and assignment of one or more persons (the "risk response owner") to take responsibility for each agreed-to and funded risk response. Risk Response Planning addresses the risks by their priority, inserting resources and activities into the budget, schedule and project management plan, as needed. Also, planned risk responses must be suitable to the implication of the risk, cost effective, timely and realistic within the project context, agreed upon by all parties involved and owned by a responsible person. Selecting the best risk response from several options is often required.

Planning involves developing actions to address individual risk, prioritizing risk actions and creating an integrated RM plan. The goal will include: 1) Reduction of the probability that a risk will occur, 2) Reduction of magnitude of loss, or 3) Change of the consequence of a risk [36]. The process output according are simple rules, process controls, testing, modeling and inheritance to [38]. The team during this process shares their knowledge on selecting the best alternative for risk treatment in risk action requests. Whenever a risk treatment alternative is recommended in a risk action request, an evaluation shall be made by the stakeholders to determine if the risk is acceptable. If the stakeholders determine that actions should be taken to make a risk acceptable, then a risk treatment alternative shall be implemented, supported by the necessary resources, and monitored and coordinated with other project activities [35]. Moreover, Knowledge Sharing helps the team in Risk Analysis process to identify possible preventive actions for the threats and enhancement actions for the opportunities. Furthermore, it is important to analyze the strategy of risk treatment adopted in similar projects and verify the efficiency of control and contingency actions that were planned. This way, the manager learns from the facts of former projects, avoiding the recurrence of problems and reusing actions which were previously successful in the risk mitigation or contingency [39].

2.4 KM and risk monitoring

Risk Monitoring is the process of identifying, analyzing, and planning for newly arising risks, keeping track of the identified risks and those on the watch list, reanalyzing existing risks, monitoring trigger conditions for contingency plans, monitoring residual risks and reviewing the execution of risk responses while evaluating their effectiveness [37].The monitoring process continues to ensure that the assessment and handling procedures are effective and, if so, that the corrective action and strategy are working. If any of these proves to be negative, the risk may need to be reanalyzed or a new handling strategy may need to be adopted. Risks may also be removed only from the project if their chance of occurrence has passed or if they have been dealt with [18]. Removing the risk from the project doesn't mean no documentation is preformed for future reference.

Also, Risk Monitoring might require altering the current execution plan, ending the risk or even initiating a contingency plan if the current plan is found to be ineffective and requires starting from the beginning of the risk process if a new risk has been identified[17] (Perera & Holsomback, 2005). This might require starting from Risk Identification, which in turn needs to communicate with KBRC for further analysis and examination. Furthermore, Risk Monitoring can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project plan. The risk response owner reports occasionally to the project manager on the effectiveness of the plan, any unanticipated effects, and any mid-course correction needed to handle the risk appropriately. Risk Monitoring also includes updating the organizational process assets, including project lessons-learned repositories and RM templates for the benefit of future projects [37]. Three steps are important to monitor risk performance:

- Monitor risk throughout the life cycle for changes in their state using measures that will be recorded in the project risk profile.
- Measures shall be implemented and monitored to evaluate the effectiveness of risk controls. The cause of an ineffective control should be identified and remedied promptly. Criteria should be set by the team to determine when a risk is no longer needed to be monitored for control effectiveness.
- The system shall be continuously monitored for new risks and sources throughout its life cycle. New risks and sources shall be communicated to the stakeholders after risk analysis.

Any monitor and review process should determine whether improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks. Consequently, Risk Monitoring can be evaluated by the KBRE process occasionally typically every bi-week According to Institute of Risk Management [40].

The importance of Knowledge Evaluation is by providing an assessment for Risk Execution and Monitoring processes. This Knowledge Evaluation might result in enriching the repository with new information, modifying existing activities, identifying or retiring risks and providing a valuable feedback on the progress of RM project. It is important to understand that risk monitoring is intended to be a daily, on-going process across the entire project lifecycle. Project team members and stakeholders should be encouraged to be vigilant in looking for risk symptoms, as well as for new project risks. Newly identified risks and symptoms of previously identified risks should be communicated immediately for evaluation and/or action. In this process, Risk Monitoring is viewed as a feedback process for the purpose of reevaluating recent results of Risk Execution concerning certain risk. The purpose of Risk Monitoring is to [35]:

- Review and update the individual risk states and the RM context.
- Assess the effectiveness of risk treatment.
- Seek out new risks and sources.

3. Conclusion

This paper emphasizes the importance of applying KM and RM in the organization in relation to a different field of business. The KM might enhance the competitive advantage and the essential knowledge to the organization. On the other hand, RM is concerned with identifying risks, source of risks and draw plans to minimize risks to acceptable level. Also, RM needs revolutionizing to enhance the alignment of risk with organization's strategy, improve risk response judgments, minimize process shocks and loses, better capturing of opportunities and enhanced cross-enterprise risks identification and management. It describes the different types of risk encountered in IT projects and the contribution it might make to enhance the IT projects execution.

4. References

[1] E. Kutsch and M. Hall, "Intervening conditions on the management of project risk: Dealing with uncertainty in information technology projects," *International Journal of Project Management*, vol. 23, pp. 591–599, 2005.

[2] ,J. Voetsch, F. Cioffi, and T. Anbari, "Project risk management practices and their association with reported project success," in 6th IRNOP Project Research Conference, Turku, Finland, 2004, pp. 680–697.

[3] L. Bannerman, "Risk and risk management in software projects: a reassessment," *Journal of Systems and Software*,

81, vol. 81, no. 12, pp. 2118–2133, 2008.

[4] K. Bakker, A. Boonstra, and H. Wortmann, “Risk management affecting IS/IT Project success through communicative action," *Project Management Journal*, vol. 42, no. 3, pp. 75-90, 2010.

[5] H. Knight. (1921). Risk. *Uncertainty and Profit.* [Online]. Available: www.econlib.org/library/Knight/knRUP.html

[6] P. Massingham, "Knowledge risk management: a framework," *Journal of Knowledge Management*, vol. 14, no. 3, pp. 464-485, 2010.

[7] E. Kutsch and M. Hall, "Intervening conditions on the management of project risk: Dealing with uncertainty in information technology projects," *International Journal of Project Management*, vol. 23, pp. 591–599, 2005.

[8] Rodriguez, E and Edwards, J S, "Before and after modelling: Risk knowledge management is required.," in IN Enterprise Risk Management Symposium Society of Actuaries, Schaumberg, IL, USA, 2008, pp. 1-23.

[9] J. Shaw, "Managing All your Enterprise's Risk.," Risk M anagement, vol. 52, no. 9, pp. 22-30, 2005.

[10] Karadsheh, L., Mansour, E., AlHawari, S., Azar, G., and El-Bathy, N., "A Theoretical Framework for Knowledge Management Process: Towards Improving Knowledge Performance," Journal of Communications of the IBIMA, pp. 67-79, 2009.

[11] D. Neef, "Managing Corporate Risk through Better Knowledge Management," Journal of The Learning Organization, vol. 12, no. 2, pp. 112-124, 2005.

[12] Fuller, M. A., Valacich, J.S., and George, J. F, Information Systems Project. New Jersey: Pearson Prentice Hall, , 2008.

[13] K. Schwalbe, Information Technology Project Management, 5th ed.: Course Technology Thomson Learning., 2007.

[14] J. Owen, "Integrating Knowledge Management with Programme Management," in *Current Issues in Knowledge Management: Information Science Reference*, 2006, pp. 132-148.

[15] H. Jones, "Risking Knowledge Management: An information Audit of Risk Management Activities within the Hobart City Council," *Journal of Library Management*, vol. 26, no. 6/7, pp. 397-407, 2005.

[16] F. Caldwell, "Risk Intelligence: Applying KM to Information Risk Management," *Journal of VINE*, vol. 38, no. 2, pp. 163-166, 2008.

[17] J. Holsomback and J. Perera, "An integrated risk management tool and process," in Aerospace Conference, 2005 *IEEE*, Big Sky, Montana, 2005, pp. 129-136.

[18] J. Tah and V. Carr, "Knowledge-based approach to construction project risk management," *Journal Of Computing in Civil Engineering*, vol. 15, pp. 170-177, 2001.

[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] Tchankova, "risk identification –basic stage in risk management," *Environmental management and health*, vol. 13, no. 3, pp. 290-297, 2002.

[21] B. Shao and K. Wu, "An integrated risk management model for financial banks with knowledge management," in 3rd International Symposium on Knowledge Acquisition and Modeling. *IEEE*, 2010.

[22] H. Jones, "Risking knowledge management An information audit of risk management activities within the Hobart City Council," *Library Management*, vol. 26, no. 6/7, pp. 397-407, 2005.

[23] R. Williams, B. Bertsch, B. Dale, T. Wiele, J. Iwaarden, M. Smith, and R Visser, "Quality and risk management: What are the key issues?" *The TQM Magazine*, vol. 18, pp. 67-86, 2006.

[24] J. Holm, "Capturing the spirit of knowledge management," *The American Conference on Information Systems*, pp. 3-5, 2001.

[25] L and Ho ïnsten, B, Ehrengren, "Performance and risk management in strategic cooperation A comparative study of business and military sectors," *International Journal of Productivity and Performance Management,* vol. 60, pp. 387-403, 2011.

[26] A. Fuller, S. Valacich, and F. George, *Information Systems Project Management: A Process and Team Approach*,

1st ed.: rentice Hall, 2008.

[27] K., Schwalbe, *Information Technology Project Management*, 5th ed.: Course Technology, Thomson Learning., 2007.

[28] P. Shedden, R. Scheepers, W. Smith, and A. Ahmad, "Towards a knowledge perspective in information security risk assessments – an illustrative case study," in *Proceedings of 20th Australasian Conference on Information Systems ACIS*, 2009.

[29] D. F. Braber, I. Hogganvik, S. Lund, K. Stolen, and F. Vrallsen, "Model-based security analysis in seven steps – a guided tour to the CORAS method," *BT Technology Journal*, vol. 25, pp. 101-17, 2007.

[30] I. Sommerville, *Software Engineering*, 8th ed. University of St. Andrews, United Kingdom: Addison-Wesley, 2006.

[31] H. Bing-hua and S. Guo-fang, "Knowledge management and data mining for supply chain risk management," *International Conference on Management and Service Science, IEEE*, 2009.

[32] S. Maguire, "Identifying risks during information system development: managing the process," *Information Management and Computer Security*, vol. 10, no. 3, pp. 126-137, 2002.

[33] R Higuera and Y. Haimes, "Software risk management," Software Engineering Institute Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, Technical Report CMU/SEI-96-TR-012 ESC-TR-96-012, 1996.

[34] L. Karadsheh, S. Alhawari, N. El-Bathy, and W. Hadi, "Incorporating knowledge management and risk management as a single process," Las Vegas, NV, USA, 2008.

[35] 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.

[36] M. Bruckner, B. List, and J. Schiefer, "Risk-Management for Data Warehouse Systems," Data Warehousing and Knowledge, pp. 219-229, 2001.

[37] I Project Management Institute, *A Guide to the Project Management Body of Knowledge: PMBOK Guide*, pp. 380, 2004.

[38] M. Beck, L. Drennan, and A. Higgins, Managing E-Risk: Asscoiation of British Insurers, Beck, M., Drennan, L., & Higgins, A. (2002), London, ISBN: 10903193-23-0, 2002.

[39] L. Farias, G. Travassos, and A. Rocha, "Managing organizational risk knowledge," *Journal of Universal Computer Science*, pp. 103-110, 2003.

[40] IRM, "A risk management standard," The Institute of Risk Management (IRM),The Association of Insurance and Risk Managers (AIRMIC) and ALARM The National Forum for Risk Management in the Public Sector, London, IRM/ALARM/AIRMIC., 2002.